جامعة الشرق الأوسط
MIDDLE EAST UNIVERSITY

مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني مع الأحكام العامة للجريمة

The extent of compatibility of the information system crimes provisions with the general provisions of crimes in the Jordanian law

إعداد الطالب

بهاء فهمي الكببجي

إشراف الأستاذ الدكتور

محمد الجبور

قدمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة الماجستير في

القانون العام

قسم القانون العام

كلية الحقوق

جامعة الشرق الأوسط

2013

بسم الله الرحمن الرحيم

{وَقُلِ اعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ}

صدق الله العظيم

سورة التوبة: الآية 105

ج

تفويض

أنا بهاء فهمي عبد الحفيظ الكببجي أفوض جامعة الشرق الأوسط بتزويد نسخ من رسالتي ورقياً وإلكترونياً للمكتبات أو المنظمات أو الهيئات والمؤسسات المعنية بالأبحاث والدراسات العلمية عند طلبها.

الإسم: بهاء فهمي عبد الحفيظ الكببجي.

التاريخ: ٢٠١٣/٥/٢٩

التوقيع: ....

د

قرار لجنة المناقشة

نوقشت هذه الرسالة وعنوانها "مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني مع الأحكام العامة للجريمة" وأجيزت بتاريخ 11 / 5 / 2013

أعضاء لجنة المناقشة.

1. أ.د محمد عودة الجبور مشرفاً ورئيساً جامعة الشرق الأوسط التوقيع..............
2. د.نغم اسحق خوشابا عضواً جامعة الشرق الأوسط التوقيع..............
3. د.فهد يوسف الكساسبه ممتحناً خارجياً جامعة عمان العربية التوقيع..............

الشكر والتقدير

أشكر الله الذي يسر أمري وسهل دربي وهداني إلى طريق العلم فالحمد لله والشكر لله.

ولا يسعني إلا أن أتقدم بجزيل الشكر والامتنان إلى الأستاذ الدكتور محمد الجبور الذي تفضل بالإشراف على رسالتي وقدم لي كل ما لديه من معلومات أسهمت في إثراء الرسالة ولم يبخل علي بوقته وجهده فجزاه الله عنا كل خير فله كل التقدير والاحترام.

كما أتقدم بالشكر إلى أعضاء لجنة المناقشة والى جميع أعضاء الهيئة التدريسية في كلية الحقوق والى كل من ساعد على إتمام هذه الرسالة وقدم لي العون والمساعدة وزودني بالمعلومات اللازمة لإتمامها .

الباحث

الإهداء

إلى مثلي الأعلى...وقدوتي في الحياة

والدي العزيز

إلى ملاكي في الحياة.. إلى من كان دعائها سر نجاحي.. إلى أغلى الحبايب

والدتي الحبيبة

إلى مربية الأجيال ونبع المحبة والعطاء

عمتي الغالية

إلى من اظهروا لي ما هو أجمل من الحياة

اخوتى وأخواتي

والى من أحب

فهرس المحتويات

الملخص باللغة العربية

عالجت هذه الدراسة مدى التوافق ما بين الأحكام التي جاء بها قانون جرائم أنظمة المعلومات المؤقت رقم (30) لسنة 2010 مع الأحكام العامة للجريمة في القوانين النافذة, وابراز دور هذا القانون في معالجة الجريمة المعلوماتية , وبيان مدى إعمال النصوص التقليدية على ما يقع من جرائم معلوماتية , وتطرقنا في الفصل الأول الى تعريف الجريمة وتحديد مشكلة الدراسة و وأهدافها و اهميتها واسئلة الدراسة وحدودها والنهج المعتمد في اعداد هذه الدراسة الا وهو المنهج الوصفي التحليلي لنصوص قانون جرائم انظمة المعلومات.

ثم تناولنا في الفصل الثاني الجرائم التي يكون فيها النظام المعلوماتي محلاً للإعتداء, وتناولنا تحديداً جرائم الدخول غير المشروع إلى نظام المعلومات وجريمة إدخال ونشر برامج ضارة التي تهدف إلى تعطيل عمل نظام المعلومات والإضرار بالغير وجريمة الحصول على معلومات تتعلق بالغير عن طريق الالتقاط غير المشروع للبيانات, حيث يعتمد هذا السلوك على اختراق الجاني لأنظمة المعلومات أو إدخال ونشر برامج خبيثة بهدف الاعتراض على الرسائل المنقولة عبر شبكة الانترنت والتصنت على المراسلات الإلكترونية أو سرقة المعلومات الخاصة ببطاقات الائتمان,والتطرق الى الركن المادي والمعنوي لهذه الجرائم والتي عالجتها المواد من (3) إلى (6) من قانون جرائم أنظمة المعلومات.

ثم تناولنا في الفصل الثالث أهم الجرائم الخاصة بالأعمال المنافية للآداب والأخلاق العامة, حيث استعمل الجناة نظم المعلومات والشبكة المعلوماتية كوسيله وأداة لارتكاب جرائمهم ومنها جرائم الاستغلال الجنسي للأطفال عبر الإنترنت وجرائم الترويج للدعارة, حيث تكلمنا عنها بإستفاضه في هذا الفصل وبينا موقف المشرع الأردني منها في المواد (8) و(9) من قانون

جرائم أنظمة المعلومات ومدى إعمال نصوص المواد الأخرى في القوانين النافذة من هذه الجريمة

ثم تناولنا في الفصل الرابع جرائم الإرهاب والجرائم ألواقعه على أمن الدولة, حيث أصبحت الشبكة المعلوماتية ملاذاً آمناً للجماعات الإرهابية والمتطرفة لتنفيذ أعمالهم الإجرامية والتخطيط لها, كما بينا أركان هذه الجرائم وخصائصها والأحكام الموضوعية التي جاء بها قانون جرائم أنظمة المعلومات في المواد (10) و(11) ومقارنتها مع الأحكام العامة للجريمة لبيان مدى انطباق النص التقليدي على هذه الجرائم.

أما الفصل الخامس والأخير فبحثنا فيه عن الأحكام الإجرائية والموضوعية التي جاء بها قانون جرائم أنظمة المعلومات في المواد من (12) إلى (16) والمادة (7) الخاصة بتشديد العقوبة, حيث بينا مدى إعمال هذه النصوص مع الأحكام التقليدية في القوانين النافذة وخاصة قانون أصول المحاكمات الجزائية, كما أوضحنا حالات تشديد العقوبة على مرتكبي الجرائم المعلوماتية كحالة التكرار أو حالة استغلال الوظيفة لارتكاب هذه الجريمة, وإجراءات الضابطة العدلية كالتفتيش والضبط والمصادرة ومدى اختصاص القضاء الأردني في حال ارتكبت إحدى الجرائم المعلوماتية.

Abstract

The current study dealt with the range of compatibility between the provisions of Information Systems Crimes Law and the general provisions of the laws in force, where the current study addressed the identification of this crime and determined its material and moral pillars as well as some of the features of such crimes.

In the second chapter , the current study addressed the crimes in which the information system is violated ,as the current study particularly dealt with the illegal access to an information system as well as the spread of harmful software that aim to harm and damage the information system and harm others.

The other crime the current study dealt with is the acquisition of others' information via illegal access and acquisition of data ,where such act depends on the penetration of information system or the spread of viruses in order to Intercept the messages transmitted by the Internet or to eavesdrop on electronic correspondence and data relating to credit cards theft. These crimes were dealt with by Articles from (3) to (6) of Information Systems Crimes Law as well as the provisions of other articles of other applicable laws regarding this crime.

Chapter four of the current study dealt with terrorism crimes and the crimes targeting state's security ,whereas internet became a safe haven for terrorist and extremist groups to carry out and plan their criminal acts. Chapter four dealt with these crimes ,their features and the objective provisions set forth by Information Systems Crimes Law in Articles (10) and (11) compared to the general provisions of the crime to identify the extent to which the traditional provisions of law are compatible in these crimes.

The last chapter, chapter five , dealt with procedural and objective provisions of the Information Systems Crimes Law represented by Articles (12),(16) and (7) regarding to intensify punishment, as we clarified the extent to which these provisions are compatible with the traditional provisions of applicable laws particularly Criminal Procedural Law. Chapter five identified the cases in which the punishment is intensified in case of repetition of the crime, exploitation the job or position to commit this crime, and judicial proceedings such as search and seizure and the extent of the Jordanian jurisdiction competence in the event of the commission of information systems related crime

الفصل الأول

مقدمة الدراسة

تمهيد :

لا يخفى أن كل تطور تقني تكون له انعكاساته على المستوى القانوني بصفة عامة وفي إطار القانون الجنائي على وجه الخصوص، وقد صاحب الانتشار الواسع لاستخدام الحاسبات نمواً مطرداً في الجرائم المرافقة لهذا الإستخدام خاصة أنها باتت تتحكم في كافة مناحي الحياة و أضحت بذاتها ضرورة ملحة لا يمكن الإستغناء عنها ، وهنا تظهر مشكلة الحاسبات الآلية فهي تتمثل في تحقيق التوازن بين مصلحة المجتمع في الحاجة إلى هذه التقنية والاستعانة بها ومصلحة الإنسان في حماية حياته الخاصة والحفاظ على أسراره وأمواله [1] .

ومن الثابت أن النشاط المعادي للمجتمع قد اقتحمته نوع جديد من المجرمين بجانب المجرم التقليدي الذي عهدناه في الماضي والذي لا زالت تقتصر جرائمه على أبعادها الفردية والاجتماعية، فقد أفرز التطور العلمي والتكنولوجي الحديث نماذج جديدة من السلوك الإجرامي تبدو النصوص القائمة والتي وضعت لمواجهة الجريمة في ثوبها التقليدي عاجزة عن استيعاب هذه الجرائم المعلوماتية ، وحيث أن الجريمة المعلوماتية ظاهرة مستجدة تطلبَ من المشرع التنبه لأهمية وحجم المخاطر والخسائر الناتجة عنها.

وقد أسفرت محاولات تطبيق نصوص التشريعات التقليدية على هذه الأنماط المستحدثة من الإجرام عن كثير من المشكلات القانونية، وتضاربت أحكام القضاء في البلد الواحد, فصدرت

---

[1] عفيفي، كامل عفيفي (2003) . **جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون**. بيروت: منشورات الحلبي الحقوقية . ص7.

أحكامً تطبق النصوص التقليدية على أي فعل ينطوي على اعتداء على أنظمة المعلومات و الحاسوب في حين اعتبرته أحكاماً أخرى فعلاً مباحاً لم يرد بشأنه نص يجرمه .

وقد أطلق الفقهاء على هذه الجريمة مسميات كثيرة فهي تسمى بجريمة الكمبيوتر والإنترنت و الجريمة المعلوماتية والبعض الآخر يطلق عليها الجريمة الإلكترونية وهناك من يطلق عليها الجريمة المستحدثة.

كما قسم فقهاء القانون الجرائم المعلوماتية إلى نوعين رئيسين هما :

الجرائم التي ترتكب باستخدام وسائل الكترونية والجرائم التي تستهدف الوسائل الالكترونية,

وتختلف الجرائم المعلوماتية بين دولة وأخرى حسب سرعة تطور المجتمعات وبنيتها وحسب قدرة المشرعين في احتواء التقدم الحاصل ضمن إطار قانوني صحيح تحسباً لأي استغلال ضار للتطور التكنولوجي الحاصل في المجتمع. [1]

وأصبحت الجريمة المعلوماتية تتمتع بعناصر تميزها عن الجريمة التقليدية سواءً من حيث أركانها والوسائل المستخدمة ومكان ارتكابها والمحل الذي وقع علية الإعتداء، فضلاً على أن نطاق الجريمة المعلوماتية يبلغ مدى أوسع من نطاق الجريمة التقليدية لانعدام الحدود الجغرافية وانعدام القيود على الحركة في الشبكة المعلوماتية, ومن تلك المستجدات تولدت الحاجة إلى إيجاد آلية قانونية لمعالجة النقص التشريعي في نطاق أنظمة المعلومات .

وكما هو مطلوب من المشرع مواكبة التطورات والمستجدات لسد الثغرات القانونية فقد حاول

---

[1] ابراهيم ، خالد ممدوح (2009) . **الجرائم المعلوماتية** .ط1.الاسكندرية : دار الفكر الجامعي. ص72.

المشرع الأردني في المادة الخامسة من قانون أصول المحاكمات الجزائية رقم (9) لسنة 1961 والمعدل بالقانون رقم (19) لسنة 2009 أن يتعاطى مع مسألة اختصاص المحاكم الجزائية بنظر الجريمة الإلكترونية، كما بادر بإحداث تعديلات على قانون المطبوعات والنشر رقم (8) لسنة 1998 وقوانين الملكية الفكرية واستحداث قانون المعاملات الإلكترونية المؤقت رقم (85) لسنة 2001 إلا أنه وجد أن هذا القدر من ملاحقة التطورات والاستخدامات الإلكترونية غير كافٍ وأن هذا التعديل لا يفي بالغرض.

وفي عام 2010 بادر المشرع الأردني بوضع قانون خاص هو قانون جرائم أنظمة المعلومات المؤقت رقم (30) لسنة (2010) ويعالج هذا القانون بشكل أساسي بعض الجرائم الإلكترونية التي تطورت وأصبحت لها مصطلحات قانونية تميزها عن الجرائم التقليدية والتي لا تجرمها التشريعات التقليدية، كما يعالج هذا القانون بعض الجرائم التقليدية التي نصت عليها التشريعات النافذة والتي تم ارتكابها عبر أنظمة المعلومات, فقد نص على تجريم فاعلها بارتكابها أو الاشتراك أو التحريض على ارتكابها بواسطة أنظمة المعلومات والحاسبات الآلية، ومن الجرائم التي عالجتها التشريعات النافذة ولم يعالجها قانون جرائم أنظمة المعلومات الجرائم المتعلقة بحقوق المؤلف والجرائم التي ترتكب بوسائل مادية ولو كان محل الجريمة يتضمن عناصر إلكترونية.

كما يرتكن هذا النوع من الإجرام على محورين أولهما ضد المال والثاني ضد الأشخاص – الطبيعية والاعتبارية– ويستمد نشاطه من القدرات الهائلة للحاسب الآلي.[1]

[1] يوسف ، امير فرج (2008) . **الجرائم المعلوماتية على شبكة الانترنت** . الاسكندرية : دار المطبوعات الجامعية . ص 215

مشكلة الدراسة:

تأتي مشكلة الدراسة في :

(دراسة مدى توافق أحكام جرائم أنظمة المعلومات مع الأحكام العامة للجريمة في القانون الأردني ودور قانون جرائم أنظمة المعلومات لمكافحة هذه الجريمة).

عناصر مشكلة الدراسة:

- دراسة مدى تطبيق نصوص قانون جرائم أنظمة المعلومات على الجرائم التي ترتكب بوسائل مادية.
- إظهار الفروق القائمة ما بين الجريمة التقليدية و الجريمة المعلوماتية.
- بيان مدى توافق الأركان الخاصة بالجريمة المعلوماتية مع الأركان العامة المشتركة للجرائم ونطاق إعمال كل منها.

أهداف الدراسة:

- تهدف هذه الدراسة إلى رصد الطبيعة الخاصة لجرائم أنظمة المعلومات بالكشف عن الجوانب المختلفة المحيطة بها .
- والبحث في النظام القانوني المطبق في المملكة الأردنية الهاشمية بالنسبة لما يرتكب من جرائم باستخدام تقنية أنظمة المعلومات .
- وإبراز أهمية وجود قانون جرائم أنظمة المعلومات في سد الثغرات والنواقص في المنظومة التشريعية .
- وبيان مدى صلاحية النصوص القانونية التقليدية في الإحاطة بجوانب الجريمة المعلوماتية .

أهمية الدراسة:

تكمن أهمية هذه الدراسة بسبب الاعتماد شبه الكامل على أجهزة الحاسب الآلي وأنظمة المعلومات في شتى مجالات الحياة, حيث أصبحت ضرورة ملحة لا يمكن الإستغناء عنها .

تكمن الأهمية فيما يلي :

- تحول نطاق الخدمة العادية إلى نطاق الخدمة الإلكترونية ومنها المعاملات التجارية والحكومية .

- ومع ازدياد دور أنظمة المعلومات وتعاظمه, أصبح من الأهمية البحث في الإطار القانوني للسعي نحو تطوير الخدمة الإلكترونية وبث الثقة والأمان في استعمال أنظمة المعلومات .
- التصدي للجريمة المعلوماتية وذلك لاتصافها بالاستمرار والتجديد في أنشطتها, فهي غير ثابتة .
- الدراسة المقدمة سوف يستفيد منها جميع مستخدمي الأنظمة التقنية في المؤسسات العامة والخاصة والشركات والبنوك ومستخدمو شبكات الإنترنت .
- كما تنبع أهميتها من حاجة المجتمع الأردني، الى إلقاء الضوء على مثل هذا النوع من الجرائم الذي يحمل الكثير من الآثار السلبية، التي تهدد أمن المجتمع و سلامته.

أسئلة الدراسة:

- ما أركان الجريمة الإلكترونية ؟
- ما مدى تطبيق نصوص قانون جرائم أنظمة المعلومات على الجرائم التي ترتكب بوسائل مادية ؟
- ما مظاهر الفروق القائمة بين الجريمة التقليدية و الجريمة الإلكترونية المستحدثة؟
- ما مدى توافق الأركان الخاصة للجريمة الإلكترونية مع الأركان العامة المشتركة للجرائم ؟
- هل قانون جرائم أنظمة المعلومات جاء بسياسه جديده من التجريم و العقاب ؟ وهل أحاط بالجريمة المستحدثة من كافة جوانبها؟

- هل جاء قانون جرائم أنظمة المعلومات لتجريم أفعال يعتقد المشرع الأردني أنها جرائم خاصة بأنظمة المعلومات وقد جرمت سلفاً في القوانين التقليدية؟ وهل ستثار مشكلة تنازع القوانين؟
- ما هو مدى الاختصاص القضائي الأردني في حال ارتكاب جريمة إلكترونية خارج حدود المملكة؟ و كيف حسم المشرع الأردني هذه المسألة؟

حدود الدراسة:

من المعلوم أن الجرائم الإلكترونية لا تحدها حدود فهي تمتد لتشمل مناطق جغرافية خارج حدود الدولة, حيث يصل مداها ليشمل دولً أخرى, كذلك يختلف نطاق التجريم والعقاب بين قوانين هذه الدول .

وهذه الدراسة سوف تتطرق فقط إلى تشريعات المملكة الأردنية الهاشمية, دون أن نغفل المقارنة مع التشريعات الأخرى حين تبرز الضرورة، هذا من حيث الحيز المكاني .

أما الحدود الزمانية للدراسة فهي تبدأ من عام 1960 حين أقر قانون العقوبات رقم (16) وصولاً إلى قانون جرائم أنظمة المعلومات المؤقت رقم (30) لسنة (2010).

فبهذا يكون الحيز الزمني لهذه الدراسة من عام 1960 حتى عام 2010 وكذلك الوقوف على الاجتهادات القضائية إلى لحظة الانتهاء من إعداد الرسالة.

محددات الدراسة:

ستركز هذه الدراسة على البحث في النظام القانوني والتشريعات المطبقة في المملكة الأردنية الهاشمية فيما يتعلق بتطور أساليب الإجرام, دون التطرق إلى القوانين المقارنة بشكل أساسي، كما لن تتطرق هذه الدراسة إلى الجوانب الفنية والتقنية لأنظمة المعلومات لأن موضوعها قانوني يأتي على أساس المقارنة بين الجرائم التقليدية والمستحدثة الواردة في قانون جرائم أنظمة المعلومات الأردني المؤقت لعام 2010 ، وذلك للخصوصية التي تتميز بها الجريمة المعلوماتية المستحدثة عن الجرائم التقليدية.

مصطلحات الدراسة:

نلاحظ انه من خلال الكتابات والأبحاث والدراسات التي أجريت انه يصعب إيجاد مصطلح موحد للدلالة على جرائم أنظمة المعلومات, مما أدى إلى القول بأن هذه الجريمة مستعصية عن التعريف بعد المحاولات العديدة التي بذلت, وأنها لم تصل حسب الزاوية التي نركز عليها إلى تعريف موحد ، ويمكن تصنيف تعريف الجريمة المعلوماتية إلى ما يلي .

أولا : تعريفات مرتبطة بالحاسب

فقد عرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها: الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً, كما عرفت بأنها : جرائم إساءة استخدام الحاسبات معتبراً أن هذا التعسف ما هو إلا فعل إجرامي يتصل بتقنية المعلومات يؤدي إلى تكبد المجني عليه خسارة و يحقق الفاعل ربحاً متعمداً.[1]

[1] حجازي،عبد الفتاح بيومي (2007) . **مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي** .الاسكندرية : دار الكتب القانونية ص 24

ثانياً : تعريفات مرتبطة بموضوع الجريمة .

يرى واضعو هذه التعريفات أن الجريمة المعلوماتية ليست هي التي يكون النظام المعلوماتي أداه لارتكابها بل هي التي تقع على النظام أو داخل نطاقه, كما عرفوها بأنها :نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل النظام أو التي تحول عن طريقه.[1]

ثالثاً: التعريف المضيق والتعريف الموسع للجريمة المعلوماتية.

بذل الفقه جهوداً كبيرة لمحاولة وضع تعريف محدد للجريمة المعلوماتية مما أدى لانقسام الفقه إلى اتجاهين, الاتجاه الأول يوسع من مفهوم الجريمة المعلوماتية والاتجاه الثاني يضيقها.

ومن التعريفات التي وضعها أصحاب الاتجاه الموسع بأنها: سلوك إجرامي يتم بمساعدة الكمبيوتر أو هي كل جريمة تتم في محيط أجهزة الكمبيوتر.

بينما عرفها أصحاب الاتجاه المضيق بأنها: كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقد كبير لازما لارتكابه من ناحية وملاحقته من ناحية أخرى كما عرفوها بأنها : هي التي تقع على جهاز الكمبيوتر أو داخل نطاقه فقط .[2]

الجريمة التقليدية :

هي كل فعل أو امتناع يشكل خروجاً على نص من نصوص التجريم يرتب له المشرع عقوبة جزائية، سواء أكان النص المعتبر وارداً ضمن نصوص قانون العقوبات العام و هو القانون رقم 16 لسنة 1960 وتعديلاته والقوانين الأخرى ذات الصلة، أو في أي قانون جزائي آخر.[1]

---

[1] الملط,أحمد خليفة(2006).**الجرائم المعلوماتية**,ط2.الاسكندرية:دار الفكر الجامعي.ص 86

[2] ابراهيم ، خالد ممدوح ,مرجع سابق.ص74

نظام المعلومات:

مجموعة البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونياً، أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو إداراتها .[2]

البيانات:

الأرقام والحروف والرموز والأشكال والأصوات والصور التي ليس لها دلالة بذاتها .[3]

الموقع الالكتروني:

مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد .[4]

التصريح :

الإذن الممنوح من صاحب العلاقة إلى شخص أو أكثر أو للجمهور للدخول إلى أو استخدام نظام المعلومات أو موقع الكتروني أو الشبكة المعلوماتية بقصد الاطلاع أو إلغاء أو حذف أو إضافة أو تغيير أو إعادة نشر بيانات أو معلومات أو حجب الوصول إليها أو إيقاف عمل الأجهزة أو تغيير موقع الكتروني أو إلغائه أو تعديل محتوياته [5].

الدخول غير المصرح به :

ينصرف معنى (الدخول) في إطار المعلوماتية بصفه عامة ليشمل كافة الأفعال التي تسمح بالولوج إلى نظام معلوماتي, ويقصد **بالدخول غير المصرح به إلى النظام**, أن توجه هجمات

[1] الزعبي،جلال محمد، و المناعسة، أسامة أحمد(2010).**جرائم تقنية نظم المعلومات الإلكترونية**،ط1.عمان:دار الثقافة.ص38
[2] المادة(2)- قانون جرائم انظمة المعلومات
[3] المادة(2)- قانون جرائم انظمة المعلومات
[4] المادة(2)- قانون جرائم انظمة المعلومات
[5] المادة(2)- قانون جرائم انظمة المعلومات

إلى معلومات الكمبيوتر أو خدماته بقصد المساس بالسرية أو المساس بالسلامة والمحتوى والتكاملية أو تعطيل القدرة والكفائه للأنظمة للقيام بأعمالها.[1]

الإطار النظري:

إن موضوع الرسالة يأتي من ناحية الربط بين الأمور الفنية والقانونية, ذلك لأن البحث في المواجهة القانونية لأنظمة المعلومات مسألة تتسم بالدقة ومن الصعوبة الإلمام بها دون البحث في الجوانب الفنية لها , وهذا ما سيكون المحور الرئيسي في الدراسه ثم نتعرف على ماهية هذه الجرائم و أحكامها وأركانها و مقارنتها بالجرائم التقليدية وبيان الأحكام المشتركة في جرائم أنظمة المعلومات والأحكام الخاصة لهذه الجريمة, وذلك من أجل الوقوف على أوجه التطابق و الاختلاف أو النقص أو الزيادة بين تلك الأركان والأحكام, والتفرقة فيما بينهم من حيث الوسائل والأركان والأدوات المستخدمة في الجريمة وطبيعتها الموضوعية.

و التكلم باستفاضة عن الدور البارز لقانون جرائم أنظمة المعلومات من ناحية تجريم هذه الأفعال للحد من تلك الجرائم, من خلال استعراض هذا القانون وبيان الجرائم التقليدية التي عالجتها التشريعات النافذه والتي تم ارتكابها باستخدام أنظمة المعلومات, وإظهار الجرائم التي لا يعالجها هذا القانون والتي عالجتها التشريعات النافذة عند ارتكابها بوسائل الكترونية.

ومن المعلوم أن قانون جرائم أنظمة المعلومات لم يعالج الجرائم التي ترتكب بوسائل مادية و لو كان محل الجريمة يتضمن عناصر الكترونية, كسرقة بطاقة ائتمان و قرص مدمج أو إتلاف جهاز كمبيوتر, كون هذا الفعل معاقب عليه في التشريعات النافذة.

---

[1] ابراهيم ، خالد ممدوح ,مرجع سابق .ص 242

و التطرق إلى دور القوانين الأخرى مثل قانون العقوبات رقم (16) لسنة 1960 و المعدل بالقانون رقم (8) لسنة 2011 وقانون المعاملات الالكترونية المؤقت رقم (85) لسنة 2001 و قانون الإتصالات رقم (13) لسنة 1995 وقانون حماية أسرار ووثائق الدولة رقم (50) لسنة 1971 و قانون منع الإرهاب رقم (55) لسنة 2006 وقانون منع الاتجار بالبشر رقم (9) لسنة (2009) وقانون أصول المحاكمات الجزائية رقم (9) لسنة 1961 من ناحية دور تلك القوانين في معالجة الجريمة المعلوماتية ومدى إحاطة هذه القوانين بجوانب الجريمة.

كذلك إظهار مدى انسجام هذه القوانين مع قانون جرائم أنظمة المعلومات ، و إظهار إذا كان هنالك تنازع فيما بينها في حال ارتكاب جريمة الكترونية.

وتبيان الفوارق فيما بينها ومدى تطبيقها، وهذا يتطلب منا تفريد نوعي للجرائم المنصوص عليها في جرائم أنظمة المعلومات وبيان صورها و استعراض أحكامها .

وكذلك اشترط أن يكون الفعل مقصودا لتجريمه, لان الغاية من وضع القانون هو منع ارتكاب الجرائم وتجنب معاقبة حسن النية.

ومن خلال البحث سوف نصل إلى بيان مدى اختصاص القضاء الأردني في حال وقوع جريمة الكترونية ولو كان النشاط الجرمي خارج المملكة .

وسيبرز لنا من خلال هذه الدراسة، ما تتطلبه الجرائم المستحدثة من شروط مفترضة أو أحكام خاصة, وبيان ما إذا كانت تصلح لأن تكون أركانا مضافة للأركان التقليدية أم لا .

الدراسات السابقة:

كان لموضوع الدراسة نصيبا من الكتب ومنها :

- إبراهيم ، خالد ممدوح (2009) . **الجرائم المعلوماتية** .ط1.الإسكندرية : دار الفكر الجامعي.

حيث تناول الجوانب التقنية للنظام المعلوماتي, فحدد مفهوم نظام المعلومات و تعريف الحاسب الآلي والنظام المعلوماتي ومكوناته, كما تحدث عن الإنترنت والجريمة المعلوماتية من حيث النشأة والتعريف والاستخدامات والملكية وإدارة الشبكة.

كما تطرق إلى المفهوم القانوني للمعلومات الإلكترونية من حيث التعريف بالمعلومة وأنواع المعلومات والشروط الواجب توافرها وطبيعتها ومصادرها والمسؤولية في مجال المعلومات ، كما تحدث في الفصل الثاني عن مفهوم الجريمة المعلوماتية وتعريفها وخصائصها ومحلها وتمييز الجريمة المعلوماتية عن الجريمة التقليدية ومكان وقوع الجريمة المعلوماتية, كما تناول أركان الجريمة المعلوماتية –الركن المادي و المعنوي– وتقسيمات الجرائم المعلوماتية ، كما تكلم عن المجرم المعلوماتي من حيث الدوافع وتصنيف أشخاص مرتكبي الجريمة المعلوماتية وأنواع المجني عليهم .

كما تناول الحديث عن الدليل الإلكتروني في الجرائم المعلوماتية, وتناول في الباب الثاني أنواع الجرائم المعلوماتية حيث تحدث في الفصل الأول عن الجرائم الواقعة على النظام المعلوماتي أما الفصل الثاني فكان عن جرائم التجارة الالكترونية.

ما تختص به الرسالة من هذا الكتاب يكمن في طبيعة الجرائم الإلكترونية وخصائصها ومحلها والمسؤولية في مجال المعلومات وأركان الجريمة المعلوماتية –الركن المادي و المعنوي– وعن المجرم المعلوماتي من حيث الدوافع و تصنيف أشخاص مرتكبي الجريمة المعلوماتية و أنواع المجني عليهم .

و ستكون دراستنا مختلفة لأنها ستبحث في النظام القانوني الأردني بشكل خاص فيما يتعلق بالجريمة المعلوماتية.

- حجازي،عبد الفتاح بيومي (2007) . **مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي** .الإسكندرية : دار الكتب القانونية .

حيث تناول التعريف بالجريمة المعلوماتية وذكر سمات المجرم الإلكتروني وخصائصه وعناصر الجريمة الإلكترونية, وتناول بعض الجرائم التقليدية التي ترتكب عبر الوسائل الإلكترونية مثل جريمة غسيل الأموال و التزوير وبيان الركن المادي لها و طرقها, كما تناول في الفصل الثاني من الباب الرابع الركن المادي في جريمة الإختراق مبينا مفهومها وصورها.

وتطرق في الفصل الأول من الباب الخامس لجريمة السرقة المعلوماتية والاختلاس والركن المادي و المعنوي للسرقة ومحلها وجاء الفصل الثاني للتحدث عن جريمة النصب التي ترتكب بوسائل الكترونية وذكر وسائل التدليس و الركن المادي لها، أما الفصل الثالث فكان للحديث عن جريمة خيانة الأمانة, كما تحدث عن جريمة الإتلاف العمدي للمعلومات وجريمة إساءة استعمال بطاقات الائتمان وجرائم الاعتداء على حرمة الحياة الخاصة .

وتبرز أهمية هذا الكتاب في الدراسة بالاستعانة بتعريف الجريمة المعلوماتية وذكر سمات المجرم الإلكتروني وخصائصه وعناصر الجريمة الإلكترونية والجرائم التقليدية التي ترتكب عبر الوسائل الالكترونية .

وستكون دراستنا مختلفة لأنها ستبحث في دور التشريعات الأردنية لعلاج و تجريم الجريمة المعلوماتية.

- الزعبي،جلال محمد، و المناعسة، أسامة أحمد(2010).**جرائم تقنية نظم المعلومات الإلكترونية**،ط1.عمان:دار الثقافة.

حيث تناول الجوانب الفنية والتقنية للحاسب الآلي, وإلى الجريمة التقليدية من حيث مفهومها وأركانها وكذلك الجريمة المستحدثة من حيث مفهومها وأطرافها وطبيعتها وخصائصها وتصنيفها, وتناول أيضاً الصبغة المالية للجريمة التقنية كجريمة إساءة الائتمان التقنية والسرقة والإتلاف والتزوير التقني وجرائم غسل الأموال التقنية وجرائم البطاقات المالية, كما تطرق إلى جرائم الإعتداء على الحياة الخاصة للأفراد وجرائم الإنترنت المتعلقة بالقاصرين وجرائم نظم الإتصالات, كما تكلم عن جريمة التجسس الإلكتروني وجريمة الإرهاب الإلكتروني وجرائم القذف الإلكتروني .

وستكون دراستنا مختلفة لأنها ستبحث في دور قانون جرائم أنظمة المعلومات لعلاج و تجريم الجريمة المعلوماتية.

- عفيفي، كامل عفيفي (2003) . **جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون.** بيروت: منشورات الحلبي الحقوقية .

حيث تطرق هذا الكتاب إلى بيان ماهية برامج وبيانات الحاسب الآلي وماهية جرائم التكنولوجيا, كما تناول موضوع الحماية الجنائية للبرامج والبيانات في إطار نصوص الملكية الفكرية ونصوص براءة الاختراع ونصوص حق المؤلف ونصوص الرقابة على المصنفات الفنية ونصوص جرائم الأموال, ونص على جرائم السرقة والنصب وخيانة الأمانة والإتلاف والتزوير, كما تطرق إلى الحماية الجنائية في إطار نصوص حماية الحياة الخاصة والحماية الجنائية للبيانات المعلوماتية من مخاطر التجسس عليها, كما تطرق إلى الدور الشرطي والقضائي في مواجهة جرائم الحاسب الآلي.

و ما تختص به الرسالة من هذا الكتاب يكمن في موضوع الحماية الجنائية للبرامج والبيانات في النصوص المذكورة أعلاه.

وستكون دراستنا مختلفة لأنها ستبحث في أركان الجريمة المعلوماتية ومدى توافقها واختلافها عن الجريمة التقليدية .

و تبرز أهمية هذا الكتاب في الدراسة بجميع ما سبق ذكره باستثناء الجوانب الفنية للحاسب الآلي .

وما تختلف به دراستنا هو التطرق لأحكام قانون جرائم أنظمة المعلومات وقانون المعاملات الإلكترونية وهذا ما لم يتطرق له هذا المرجع .

- يوسف ،أمير فرج (2008) . **الجرائم المعلوماتية على شبكة الانترنت** . الإسكندرية : دار المطبوعات الجامعية .

حيث تناول هذا الكتاب في الباب التمهيدي إلى آداب السلوك الأساسية على الإنترنت وتصنيف الجرائم حسب مواطن الاختراق وحسب مساسها بالأشخاص والأموال وتطورات ظهور الجرائم الالكترونية، كما بين في الفصل الأول منه أنواع الفيروسات وإشكالها وكيفية مواجهتها.

أما الفصل الثاني فقد تكلم عن الجرائم الإلكترونية من حيث سبل وآليات الحماية من الجريمة الإلكترونية وجرائم التجسس والإرهاب الإلكتروني، أما الفصل الثالث فقد كان عن جريمة الغش التجاري المعلوماتي, وتطرق في الفصل الرابع على مكافحة الجرائم المعلوماتية من حيث النطاق القانوني للبيئة العربية في حماية برامج الكمبيوتر وقواعد البيانات و اشكالياتها وخصوصية جرائم الكمبيوتر والإنترنت وإجراءات جمع الأدلة والتحقيق فيها، أما الفصل الخامس فقد تطرق إلى الاتفاقيات الدولية.

وما تختص به الرسالة من هذا الكتاب هو تصنيف الجرائم حسب مساسها بالأشخاص والأموال وتطورات ظهور الجريمة الالكترونية.

وستكون دراستنا مختلفة لأنها ستبحث في أركان الجريمة المعلوماتية المستحدثه ومدى توافقها واختلافها عن الجريمة التقليدية .

(ما يميز هذه الدراسة عن الدراسات السابقة هو الوقوف على أحكام قانون جرائم أنظمة المعلومات لسنة 2010 في معالجة الجريمة المعلوماتية، حيث لم أجد فيما كتب ما يبرز دور هذا القانون في معالجة الجرائم المعلوماتية).

منهجية الدراسة:

إن المنهج الذي سوف يعتمده الباحث في إعداد هذه الدراسة هو المنهج الوصفي التحليلي لنصوص قانون جرائم أنظمة المعلومات والقوانين التقليدية النافذة ووصف أركان الجريمة الإلكترونية والجريمة التقليدية, بغية تحديد الأطر العامة لتطور الجريمة في النظام القانوني الأردني.

هيكلة الدراسة:

حيث أن هذه الدراسة تنصب على قانون جرائم أنظمة المعلومات فسنخصص لتلك الصور الواردة في قانون جرائم أنظمة المعلومات الفصول التالية مقسمة على خمسة فصول, حيث يتضمن الفصل الأول: المقدمة ومشكلة الدراسة وهدف الدراسة وأهمية الدراسة وأسئلة الدراسة وفرضياتها وحدود الدراسة ومحددات الدراسة والمصطلحات الإجرائية والإطار النظري والدراسات السابقة, وتكون عناوين الفصول الأخرى كالتالي:

الفصل الثاني: جريمة الدخول إلى موقع الكتروني ونظام معلوماتي والعبث بمحتوياته.

الفصل الثالث: الجرائم الخاصة بالإعمال المنافية للآداب العامة.

الفصل الرابع: جرائم الإرهاب والإطلاع على أسرار الدولة.

الفصل الخامس: الأحكام الإجرائية والموضوعية لجرائم أنظمة المعلومات.

وسنتناول بعدها الخاتمة والنتائج والتوصيات .

الفصل الثاني

جريمة الدخول إلى موقع الكتروني ونظام معلوماتي

والعبث بمحتوياته

أضحى غزو الحاسب الآلي نتيجة وبصمة واضحة للتقدم التكنولوجي في الحياة المعاصرة حيث إن استخدام الشبكات المعلوماتية المحلية والعالمية أدى إلى تحول العالم لقرية صغيرة نتيجة ربط هذه الحاسبات بعضها ببعض عن طريق شبكات الاتصال, وبالتالي ظهرت جرائم مستحدثة ترتكب باستخدام أنظمة المعلومات, ومن بينها الدخول إلى النظام المعلوماتي الخاص بالغير والإطلاع على البيانات والمعلومات الخاصة به بدون وجهه حق.[1]

ومن خصائص الجريمة المعلوماتية أنها تقع أثناء عملية المعالجة الآلية للبيانات والمعطيات,

ففي مرحلة الإدخال حيث التعامل مع البيانات المجمعة والمجهزة يكون من السهل إدخال بيانات جديدة لا علاقة لها بالمعطيات القائمة ومحو البيانات الأساسية المطلوب إدخالها, وفي مرحلة المعالجة حيث يمكن إدخال أي تعديلات على البرنامج تحقق الهدف الإجرامي كالتلاعب في برامج النظام المعلوماتي, فيتم إدخال بيانات غير مصرح بها تكون على شكل برامج خبيثة (فيروس), أما المرحلة الأخيرة المتعلقة بالمخرجات وفيها يتم التلاعب في النتائج التي يخرجها النظام المعلوماتي بشأن بيانات صحيحة أدخلت للنظام وتمت معالجتها بطريقة غير صحيحة [2].

---

[1] عفيفي، كامل عفيفي,مرجع سابق.ص7

[2] إبراهيم .ممدوح خالد. مرجع سابق .ص84

وليس هذا فحسب, بل تمكن المجرم المعلوماتي من إدخال برامج خبيثة إلى جهاز الغير عن طريق الشبكة المعلوماتية والتي تمكنه من الاطلاع والعبث وإتلاف محتويات هذا الجهاز, وفي حالة تمكن الجاني من الدخول إلى النظام أو الموقع الإلكتروني المملوك للغير فبإمكانه القيام بالعديد من الأفعال والسلوكيات التي تشكل جريمة كالحصول على البيانات التي تتعلق ببطاقات الائتمان والاعتراض والتصنت على الرسائل والمعلومات المتبادلة في الشبكة المعلوماتية وهذه السلوكيات جرمها المشرع الأردني في قانون جرائم أنظمة المعلومات المؤقت رقم (30) لسنة 2010 في المواد (6,5,4,3) و التي سوف نتناولها في هذا الفصل.

تقسيم:

سنعمل على تقسيم هذا الفصل إلى مبحثين؛ نعرض في المبحث الأول جرائم الدخول والإدخال إلى النظام المعلوماتي وفق ما جاءت به المواد(4,3) ثم نتناول بعد ذلك في مبحث ثاني جرائم المعلومات التي تتعلق بالغير وفق ما جاءت به المواد (6,5) كالتالي:

المبحث الأول : جرائم الدخول والإدخال إلى النظام المعلوماتي.

المبحث الثاني: جريمة الحصول على معلومات تتعلق بالغير.

المبحث الأول

جرائم الدخول والإدخال إلى النظام المعلوماتي

تمهيد:

يتحقق الدخول غير المصرح به إلى جهاز الحاسوب بالوصول إلى البيانات والمعلومات والبرامج المخزنة على الدعامة الإلكترونية في جهاز الحاسوب أو الأجهزة المتصلة بالشبكة المعلوماتية ,حيث يكون هذا الدخول عنوةً ومخالف لإرادة المالك أو المسئول عن هذا النظام وبمعنى آخر يتمثل في إساءة استخدام الحاسوب ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه للوصول إلى المعلومات والبيانات المخزنة بداخله[1].

وسوف نخصص هذا المبحث للحديث عن جريمة الدخول والإدخال غير المشروع إلى النظام المعلوماتي وفق ما جاءت به المادة (3) من قانون جرائم أنظمة المعلومات رقم (30) لسنة (2010) الخاصة بالدخول, وما جاءت به المادة (4) من نفس القانون التي تعالج جرائم الإدخال أو نشر البرامج, كما سوف نتطرق إلى بيان الركن المادي والمعنوي لهذه الجرائم وموقف المشرع الأردني منها.

وعليه ارتأيت إلى تقسيم هذا المبحث كالتالي:

---

[1] إبراهيم .ممدوح خالد. مرجع سابق .ص243

المطلب الأول: جريمة الدخول والبقاء غير المصرح به لنظام المعلومات.

المطلب الثاني :جريمة ادخال أو نشر برامج بهدف الإضرار بالغير.

المطلب الأول

جريمة الدخول والبقاء غير المصرح به لنظام المعلومات

جاء المشرع الأردني بنصوص تكفل تجريم فعلي الدخول والبقاء غير المصرح به لنظام المعلومات حيث نصت المادة (3) من قانون جرائم أنظمة المعلومات المؤقت على انه:

(أ. كل من دخل قصدا إلى موقع الكتروني أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح ، يعاقب بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (100) مائة دينار ولا تزيد على (200) مائتي دينار أو بكلتا هاتين العقوبتين.

ب. إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) إلف دينار أو بكلتا هاتين العقوبتين.

تتحقق هذه الجريمة في صورتها البسيطة بمجرد فعل الدخول غير المشروع أو البقاء غير المشروع في النظام المعلوماتي مع توافر القصد الجنائي [1].

وتقع الجريمة في هذه الحالة لو حاول أي شخص ونجح في الدخول لنظام أو شبكة من خلال تجاوز تلك الضوابط وتجاوز التصريح أو انتحال صفة أو كان دخوله لتلك المؤسسة على سبيل الزيارة دون السماح له باستخدام نظام معلومات فيها أو الوصول إلى شبكة معلوماتية أو نظام معلومات فيها، فيكون دخوله معاقب عليه بموجب البند (أ) من المادة (3) بغض النظر عن الوسيلة المستخدمة طالما كان لا يملك التصريح, أو كان يملك التصريح ولكنه تجاوز الدخول المصرح به كأن يسمح له باستخدام نظام المعلومات أو الشبكة المعلوماتية لمدة معينة ولكنه بقي يشغلها مدة إضافية، أو يخالف التصريح كأن يكون مسموحا له الوصول لبعض المعلومات في الشبكة الداخلية ولكنه تجاوز ذلك ودخل قصداً إلى قسم آخر من تلك الشبكة كنظام الموظفين أو بريدهم[2].

وتتحقق هذه الجريمة في صورتها المشددة متى ترتب على فعل الدخول أو البقاء غير المشروع محو أو تعديل أو تعطيل عمل نظام المعلومات, ويكفي أن يكون هناك علاقه سببية ما بين فعل الدخول و البقاء غير المشروع وبين النتيجة التي تحققت وهي الاعتداء على البيانات أو النظام المعلوماتي ككل وهذه النتيجه هي التي اعتبرها المشرع ظرفاً مشدداً [3].

و قد شدد المشرع الأردني العقوبة في البند (ب) من المادة (3)على فعل الدخول غير المصرح به إذا كان بهدف القيام بالأفعال السالفة الذكر حيث تضمنت عقوبة مشددة لجريمة

---

[1] حجازي ,عبد الفتاح بيومي .مرجع سابق, ص364

[2] المذكرة الايضاحية لقانون جرائم أنظمة المعلومات رقم (30) لسنة (2010) , ص3

[3] حجازي ,عبد الفتاح بيومي .مرجع سابق, ص367

الدخول غير المصرح به المنصوص عليها في الفقرة (أ) من ذات المادة، حيث أن الدخول بحد ذاته جريمة معاقب عليها، فإذا كان الدخول بهدف ارتكاب أي من الأفعال أو تحقيق أي من النتائج التي ينص عليها البند (ب) موضوع البحث، فتشدد العقوبة بحق الفاعل على النحو المذكور.

وللوقوف على تلك الأفعال، فيمكن إيجازها على النحو التالي:[1]

إلغاء البيانات أو المعلومات أو حذفها أو إضافتها أو تدميرها أو إتلافها: إن المعلومات التي يختزنها النظام المعلوماتي تمثل هدفاً أساسياُ للجناة الذين يحاولون الوصول والعبث بها بشتى الطرق مما يؤدي إلى إتلاف هذه البيانات أو تدميرها والاعتداء عليها[2].

وقد تم تجريم تلك الأفعال لعدم وجود حماية قانونية صريحة للبيانات والمعلومات الالكترونية في التشريعات العقابية إضافة إلى لزوم معاملتها معاملة المال والوثائق والحقوق الأخرى التي يحظر القانون المساس بها, فالمعلومات والبيانات الالكترونية لها قيمة مادية ومعنوية لا تقل عن قيمة الوثائق والأموال والحقوق الأخرى المحمية بموجب التشريعات النافذة، ولا إمكانية لتصور وقوع إتلاف الكتروني لا يكون محله مال الكتروني معنوي وهو أمر لا يتوفر إلا في بيئه الكترونية قوامها تقنية نظم المعلومات, كما قد تحتوي هذه البيانات على دراسات ومعلومات خاصة أو أنها برامج تتحكم بأنظمة أو مؤسسات وتسيرها, مما يترتب على ما تقدم أن أي من تلك الأفعال قد ينجم عنها تعطيل خدمات مثل الكهرباء والمياه وغيرها، كما قد ينجم عنها تعطل الأجهزة ووقوع خسائر مادية أخرى، مما يتطلب وجود

---

[1] المذكرة الايضاحية لقانون جرائم أنظمة المعلومات رقم (30) لسنة (2010) , ص3
[2] الملط,أحمد خليفة,مرجع سابق.ص181

حماية تشريعية خاصة للمعلومات والبيانات المخزنة في نظام معلومات أو شبكة معلومات لسهولة الوصول إليها وإلغاءها و حذفها و إضافتها و تدميرها و إتلافها[1].

إفشاء البيانات أو المعلومات: إن الهدف من تجريم قصد إفشاء البيانات والمعلومات المنصوص عليه في البند (ب) من المادة (3) كما جاء في مشروع قانون جرائم أنظمة المعلومات هو حماية حق مالكي المعلومات والبيانات في الحفاظ على الخصوصية والسرية لمالكها، وتتركز الخصوصية على فكرة حق الشخص أن يقرر متى وكيف و إلى أي حد يمكن مشاركة معلوماته الشخصية والمهنية مع الآخرين، أما فكرة السرية فتتمحور في حق الشخص بأن يخفي المعلومات الخاصة به عن الغير ممن لا يرغب معرفتهم بتلك المعلومات سواء كانت تلك المعلومات تخص الأفراد أو المؤسسات، ويكون الفعل غير معاقب عليه متى كان غير مصرح به من صاحب العلاقة أو كان كلا من الدخول والاطلاع غير مصرح بهما، فعلى سبيل المثال لا الحصر، من كان مسموحا له بالدخول إلى نظام المعلومات لغايات إغلاق الجهاز الخاص بآخر لا يحق له الدخول إلى المعلومات والبيانات المخزنة به بقصد إفشاءها فإذا فعل ذلك فتنطبق عليه أحكام الفقرة (ب) من المادة (3) من القانون كونه تجاوز التصريح الممنوح له، ولا فرق بين التمكن من إفشاء المعلومات والبيانات أو عدمه طالما كان القصد من الدخول غير المشروع أن يقوم بإفشاء معلومات تخص الغير دون تصريح أو بما يجاوز التصريح حيث تطلب المشرع لها قصداً خاصاً[2].

حجب البيانات أو المعلومات: قد يكون حجب البيانات والمعلومات موجه نحو نظام المعلومات أو شبكة المعلومات مباشرة من خلال منع الغير من الإطلاع عليها، وتفترض هذه الحالة عدم

---

[1] الزعبي،جلال محمد، و المناعسة، أسامة أحمد,مرجع سابق,ص122
[2] المذكرة الايضاحية لقانون جرائم أنظمة المعلومات رقم (30) لسنة (2010) , ص3

إيقاع ضرر بالمعلومة ذاتها ولكن منع المستفيدين ومن لهم الحق في الوصول للمعلومات والبيانات من الوصول إليها أو استخدامها بأي شكل عبر تعطيل الوصول إليها، و تبرز أهمية التجريم بأن المؤسسات أصبحت تعتمد في تقديم خدماتها للمستفيدين على أنظمة المعلومات والشبكة المعلوماتية وإن حجب البيانات والمعلومات يعني تعطيل تقديم أو الوصول لتلك الخدمات.

توقيف أو تعطيل عمل نظام معلومات[1]: يفترض تعطيل عمل نظام المعلومات قيام الفاعل بفعل من شأنه منع النظام من العمل، سواء تم العبث ببياناته و معلوماته أم لا، والنتيجة واحدة هي عدم قدرة مستخدم النظام من القيام بأعماله الخاصة أو تقديم خدمات للغير أو غير ذلك.

تغيير بيانات أو معلومات: يقع تحت بند تغيير البيانات والمعلومات الكثير من الأفعال التي أبسطها تغيير معلومات شخصية غير ذات أهمية لتصبح غير مفهومة ولا يسبب تغييرها ضررا بأحد و تتصاعد أثر تغيير البيانات والمعلومات حتى الإضرار بمعلومات تتعلق بخدمة عامة أو أوراق مالية أو حقوق أو أموال أو رمز الدخول لنظام و تتفاوت تلك الأفعال من حيث أثرها، وتتفاوت بالتالي من حيث عقوبتها ويخضع تقدير العقوبة المناسبة لسلطة قاضي الموضوع.[2]

نقل بيانات أو معلومات: يستوي في نقل البيانات والمعلومات المخزنة في نظام معلومات أن يكون ذلك النقل داخل ذات النظام أو الأداة أو إلى نظام آخر أو أداة أخرى دون إبقاء تلك المعلومات في مكانها الأصلي، فالفعل المجرم هو نقل تلك المعلومات و البيانات و يتفاوت أثر مثل هذا النقل من حالة إلى أخرى فقد يترتب على نقل المعلومات انتهاك الخصوصية والسرية

[1] المذكرة الايضاحية لقانون جرائم أنظمة المعلومات رقم (30) لسنة (2010) , ص3
[2] المذكرة الايضاحية لقانون جرائم أنظمة المعلومات رقم (30) لسنة (2010) , ص3

وقد يترتب عليه تعطيل نظام معلومات أو شبكة معلوماتية أو عمل موقع الكتروني وقد يترتب عليه تحريف في الحقائق أو التزوير أو التجسس أو ارتكاب جريمة أخرى مثل انتحال الهوية، فمفهوم نقل البيانات و المعلومات واسع جدا و ينبغي النظر إلى أثر ذلك الفعل قبل تحديد العقوبة المناسبة، ولذلك تتفاوت العقوبة تبعا للأثر ألجرمي.

نسخ بيانات أو معلومات[1]: يفترض نسخ البيانات الحصول على نسخة من تلك البيانات أو المعلومات ونقلها أو تخزينها في أداة أو برنامج أو نظام أو طباعتها دون حذفها أو شطبها من موقعها الأصلي، وإن كان مثل هذا الفعل يشكل سرقة، إلا أن خطورة نسخ البيانات والمعلومات المخزنة بوسائل الكترونية تكمن في صعوبة كشفها وإثباتها وبالتالي تم النص صراحة على تجريمها ومعاقبتها. تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديله أو إشغاله أو انتحال صفته: تبرز أهمية تجريم الأفعال الواقعة على مواقع الكترونية هو سهولة الوصول الى تلك المواقع من خلال الشبكة المعلوماتية، وتتعدد صور تلك الأفعال ابتداء من تعطيل الموقع مؤقتا وحتى تعطيله بشكل دائم أو انتحال صفة مالكه والتعامل مع الجمهور من قبل الفاعل كما لو كان مالكا لذلك الموقع وبالتالي الإضرار بمصالح مالكه الحقيقي أو مستخدمه وحرمان من يتعامل معه من الاستفادة من ذلك الموقع الالكتروني.

ولبيان الركن المادي والمعنوي لهذه الجريمة ارتأيت الى تقسيم هذا المطلب الى فرعين كالتالي:

الفرع الأول

[1] المذكرة الايضاحية لقانون جرائم أنظمة المعلومات رقم (30) لسنة (2010) , ص3

الركن المادي في جريمة الدخول والبقاء غير المصرح به

يلزم لقيام الركن المادي في جريمة الدخول والبقاء غير المصرح به في نظام المعالجة الآلية للبيانات أن يقوم الجاني بنشاط خارجي ملموس أو فعل مادي يعبر به عن انصراف ارادته في انتهاك نظام الحماية الأمني للبيانات والمعطيات الموجودة داخل النظام, وذلك إما في الدخول المجرد لها للاطلاع عليها أو لمحاولة العبث بها أو تعديها أو إتلافها أو إفشائها والتعبير عن إرادته في البقاء داخل هذا النظام بدون وجه حق لتحقيق أحد الأهداف الإجرامية [1].

ويتمثل الركن المادي في جريمة الدخول والبقاء غير المصرح به لأنظمة المعلومات في صورتين وهما:

أولاً.**فعل الدخول (الولوج):**

تتمثل جريمة الولوج والبقاء غير المشروع في أنظمة المعالجة الآلية للبيانات في حالة اختراق(دخول) الجاني للنظام المعلوماتي بأكمله أو لجزء منه, سواءً كان جزئاً مادياً أو برامج أو مجرد بيانات مختزلة في النظام عن طريق التوصل إلى الأرقام أو الكلمات أو الشيفرات أو الحروف أو المعلومات السرية التي تكون بمثابة النظام الأمني لجهاز الحاسب الآلي أو للبرامج والنظم المعلوماتية, مع توافر القصد الجنائي لدى مرتكب الفعل وأياً كان الباعث عليه[2].

ويكون الاختراق غير المشروع الذي يحدث من قبل الجاني بأن يستعمل لوحة المفاتيح ليخترق نظام الحماية ثم الدخول إلى نظام الإتصال المرتبط بين جهاز الحاسوب وأجهزة أخرى ثم

---

[1] زين الدين,بلال أمين(2008).**جرائم نظم المعالجة الآلية للبيانات**.الاسكندرية:دار الفكر الجامعي.ص271

[2] حجازي .عبد الفتاح بيومي . مرجع سابق . ص 357

الدخول إلى نظام الغير, سواء أكان عبر شبكة الانترنت أو عبر شبكات الإتصال المحلية أو المغلقة, ويعطي لنفسه الحق في التجوال داخل نظام معلوماتي بحرية وبصورة غير مشروعة[1].

ومن صور الدخول غير المشروع أن يقوم مالك النظام بوضع قيود على الدخول لنظامه المتضمن بيانات خاصة غير متاحة للجمهور, وقيام الجاني بالدخول والإطلاع على هذه البيانات دون احترام هذه القيود, وأيضا يمكن أن يكون الدخول بتشغيل جهاز مغلق ويعد ذلك الدخول بدون وجه حق طالما تم ذلك دون موافقة صاحب الحق في ذلك أو باستعمال كمبيوتر مفتوح مملوك للغير, فقد يكون جهاز الكمبيوتر قيد الاستعمال ممن له الحق في ذلك لكنه تغافل عنه أو انشغل وقام شخص أخر باستخدامه والاطلاع على معلوماته[2].

ويثور التساؤل هنا عن مدى انطباق نص المادة (416) من قانون العقوبات والتي تجرم استعمال أشياء الغير بدون حق على ما يقع من جرائم دخول غير مصرح به إلى نظام معلوماتي مملوك للغير؟

نصت المادة(1/416)من قانون العقوبات على انه (1-كل من استعمل بدون حق شيئا يخص غيره بصورة تلحق به ضررا دون أن يكون قاصدا اختلاس ذلك الشيء ،عوقب بالحبس حتى ستة أشهر ، وبالغرامة حتى عشرين دينارا أو بإحدى هاتين العقوبتين).

باستقراء نص المادة السالفة نجد أننا أمام نص تقليدي يتطلب وجود شيء أو مال مادي حتى تقع عليه هذه الجريمة, فيمكن أن تنطبق هذه المادة في حال كانت الجريمة تقع على المكونات المادية للحاسب الآلي فقط كاستعمال (الشاشة أو لوحة المفاتيح وغيرها) بدون وجه حق, ومن

---

[1] الزعبي . جلال محمد . مرجع سابق ص 248

[2] حجازي ,عبد الفتاح بيومي .مرجع سابق, ص356

المسلم به أن البيانات والمعلومات لا تتمتع بكيان مادي ملموس, كما أن فعل الاستعمال في هذه الجريمة يفترض فعلاً يخرج به الفاعل الشيء من حيازة المجني عليه ويدخله في حيازته ليستعمله هو, الأمر الذي لا يتحقق في حالة الاستعمال غير المصرح به للنظام المعلوماتي حيث لا يمكن إعمال نص المادة (416) على المكونات المنطقية الغير ملموسه لنظام المعلومات.

كما ويتحقق الركن المادي متى دخل الجاني إلى النظام كله أو جزءٌ منه, مثل الدخول إلى طرفية الحاسب أو شبكة الاتصال أو البرامج, كما ويمكن أن يتحقق الدخول غير المصرح به إذا كان مسموحاً للشخص الدخول إلى جزء معين من النظام حيث تجاوزه إلى جزء آخر غير مسموح له بالدخول اليه[1].

وكذلك هناك صورة أخرى وهي استخدام الأرقام السرية الخاصة بالدخول إلى موقع الكتروني غير متاح للجميع, والتي يمكن التوصل إليها عن طريق الصدفة أو المحاولات المتكررة أو عن طريق سرقة كلمة السر, وهذه المواقع غالبا ما تتطلب اشتراك ودفع مبلغ من المال للاستفادة من خدماتها, وحيث يقوم الجاني بالدخول إلى هذه المواقع والإطلاع على البيانات والمعلومات الموجودة بداخله والاستفادة منها بدون وجه حق وبطريقه غير مصرح بها مما يؤدي إلى تكبد أصحابها مبالغ طائلة وخسائر مالية نتيجة هذا الدخول غير المشروع[2].

كما يلزم لقيام جريمة الدخول والبقاء غير المصرح به في أنظمة المعالجة الآلية للبيانات توافر ثلاثة شروط, يتمثل الشرط الأول في ضرورة وجود نظام معالجة آلية للبيانات أي مجموعة من الوحدات والأجهزة والبرامج التي تعمل مجتمعة بغية معالجة وإخراج و تخزين

---

[1] حجازي .عبد الفتاح بيومي . مرجع سابق.ص 357

[2] زين الدين,بلال أمين,مرجع سابق,ص262

واسترجاع البيانات عند الحاجة, و يتمثل الشرط الثاني في ضرورة وجود نظام حماية للبيانات ضد الولوج إليها, فالرأي الغالب في الفقه يرى أن نظام الحماية له دور فعال في إثبات القصد الجنائي عند الدخول, والشرط الثالث يتمثل في أن يكون الدخول أو البقاء بدون حق أو سند من القانون أو بناء على عقد أو اتفاق[1].

ثانياً.البقاء غير المشروع:

والمقصود به: التواجد من قبل الجاني داخل نظام المعالجة الآلية للبيانات والتجول بين الملفات و المجلدات والانتقال من جزء إلى آخر داخل النظام المعلوماتي وبصفة مستمرة, وهذا ما يجعل فعل البقاء (التواجد) من الأفعال المستمرة الأثر على خلاف فعل الدخول الذي يتصف بالوقتية [2].

ويتمثل فعل البقاء داخل نظام المعالجة الآلية للبيانات أيضاً عند دخول الفاعل إلى النظام بطريق الصدفة البحته أو تجاوز المدة المحددة له داخل النظام وانتفاء القصد الجنائي لديه, وتقوم الجريمة هنا عند انصراف إرادته إلى البقاء داخل النظام, حيث يعاقب الجاني عن جريمة عمديه لأن إرادته انصرفت إلى البقاء داخل نظام المعالجة الآلية رغم علمه بأن دخوله غير مشروع[3] .

كما أن البقاء داخل النظام يفترض اختلاس وقت النظام ويتخذ صورة الجريمة المستمرة, كما وجد في الفقه من يقول بأن هذه الجريمة تقوم بسلوك إجرامي سلبي عند امتناع الجاني عن

---

[1] زين الدين,بلال أمين,مرجع سابق,ص262
[2] زين الدين,بلال أمين,مرجع سابق,ص273
[3] حجازي .عبد الفتاح بيومي . مرجع سابق.ص362

الخروج من النظام بعد الدخول إليه, ومن الفقهاء من يرى وجود تعدد معنوي لهذه الجريمة[1].

و يمكن أن نميز بين ثلاثة صور لمحل جريمة الدخول والبقاء غير المصرح به, فإما أن يكون محل الجريمة المعلومات في ذاتها وإما نظم أجهزة الحاسوب غير المرتبطة فيما بينها بشبكة اتصال وإما أن يكون محلها شبكات المعلومات , فيكون النشاط المادي إما في الدخول مباشرة إلى النظام أو في اعتراض عملية الاتصال من اجل الدخول إلى هذا النظام[2].

الفرع الثاني

الركن المعنوي في جريمة الدخول والبقاء غير المصرح به

إن تفهم الركن المعنوي في جرائم الانترنت يعد من الأمور الهامة في تحديد طبيعة السلوك المرتكب وتكييف النصوص, فبدون الركن المعنوي لن يكون هنالك جريمة حيث لا تقوم الجريمة بتحقق الركن المادي فقط بل يلزم أن يتوافر الركن المعنوي أيضاً, ويعرف الركن المعنوي بأنه: النشاط الذهني والنفسي للجاني وجوهر هذا النشاط هو الإرادة الجرمية التي تربط الشخص بالفعل الذي ارتكبه,[3] ونجد أن المشرع الأردني قد اهتم بضرورة وجود الاراده والنية عند ارتكاب الجريمة فباستقراء نصوص مواد قانون جرائم أنظمة المعلومات نجدها تبدأ بعبارات مثل (كل من دخل قصداً) وعبارة (كل من قام قصداً) وعبارة (كل من استخدم قصدا) و(كل من أرسل أو نشر قصدا), وهذا ما يدل على اشتراط و جود القصد حتى تعتبر الجريمة متممه لأركانها.

---

[1] حجازي .عبد الفتاح بيومي . مرجع سابق.ص361

[2] إبراهيم , خالد ممدوح , مرجع سابق.ص258

[3] الجبور ,محمد عودة(2012).**الوسيط في قانون العقوبات**,ط1.عمان:دار وائل للنشر.ص238

وعليه فإن جريمة الدخول والبقاء في النظام المعلوماتي هي من الجرائم المقصودة التي يتطلب لقيامها القصد الجنائي وتحقق عناصره من علم و إرادة وسوف نتناول فيما يلي القصد العام ثم نتعرض للقصد الخاص في هذه الجريمة.

أولاً. القصد العام : لا بد أن يحيط الجاني علماً بأنه يقوم بفعل غير مشروع يتمثل في الدخول و البقاء في النظام المعلوماتي المملوك لغيره وغير المصرح له بدخوله, وقيامه بالدخول قصداً وبوسائل غير مشروعه كالاحتيال على النظام أو انتحال صفة المستخدم أو سرقة كلمة المرور وقد يكون الدخول أحياناً بطريق الصدفة أو السهو والخطأ, ولكن الجاني يختار البقاء في النظام مع علمه بأن دخوله غير مصرح به, وقيامه بالعديد من الأفعال التي تشكل انتهاكاً للنظام كالإطلاع على الأسرار والتنقل بين قوائم البيانات, ففي هذه الحالة يكون قد ارتكب جريمة الدخول و البقاء غير المصرح به[1].

كذلك يجب أن تتجه إرادة الجاني إلى تحقيق فعلى الدخول والبقاء وإرادة حصول النتيجة الإجرامية وهي التجوال داخل النظام, فإذا لم تتجه إرادة الجاني إلى ذلك ولكنه وجد نفسه في إطار النظام المعلوماتي عن طريق الصدفة ووقف عند هذا الحد ولم يتعدى سلوكه إلى البقاء أو التجوال أو الاطلاع أو غير ذلك أو اكره على فعل الولوج أو البقاء فلا يتوافر في هذه الحالة القصد الجنائي ولا عقاب على فعله لانتفاء القصد من ذلك.[2]

[1] زين الدين,بلال أمين,مرجع سابق,ص277
[2] زين الدين,بلال أمين,مرجع سابق,ص278

وفي حالة توافر القصد الجنائي بعنصريه العلم والإرادة فإنه لا محل للإعتداد بالباعث لارتكاب الجريمة فتقوم الجريمة في حق الجاني حتى ولو كان باعثه الفضول أو اللهو أو إثبات الذات [1].

ثانياً: القصد الخاص

تتطلب بعض نصوص تشريعات الدول المختلفة التي جرمت الدخول والبقاء غير المصرح به إلى النظام المعلوماتي توافر القصد الخاص إلى جانب القصد العام المتمثل في نية الجاني للدخول إلى النظام بهدف التجوال والاطلاع على معلومات وبيانات الغير والاعتداء عليها[2] بالإلغاء أو الحذف أو الإتلاف أو التعديل أو الحجب أو الإفشاء أو النقل أو النسخ أو بتعطيل عمل نظام معلوماتي أو موقع الكتروني, وهذا ما أورده المشرع الأردني في نص المادة (3/ب) من قانون جرائم أنظمة المعلومات.

المطلب الثاني

[1] حجازي .عبد الفتاح بيومي . مرجع سابق.ص 366
[2] إبراهيم .ممدوح خالد. مرجع سابق .ص243

جريمة إدخال أو نشر برامج بهدف الإضرار بالغير

جرمت المادة (4) من قانون جرائم أنظمة المعلومات الأفعال المتعلقة بإدخال أو نشر برامج تلحق الضرر بالغير, حيث نصت على انه: (كل من ادخل أو نشر أو استخدم قصدا برنامجا عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات، بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الغير من الاطلاع على بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول إليه أو تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه دون تصريح أو بما يجاوز أو يخالف التصريح يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا هاتين العقوبتين).

حيث عالجت هذه المادة أي مهاجمة أو تخريب لأنظمة المعلومات والشبكة المعلوماتية والمواقع الالكترونية عن طريق إدخال ونشر واستخدام برامج بقصد تحقيق أحد النتائج المبينة في البند (ب) من المادة (3), حيث لا يشترط الدخول إلى نظام الغير لإلحاق الضرر به بل يكفي استخدام برنامج عن بعد لهذه الغاية، مثل إرسال فيروس عبر البريد الالكتروني أو استخدام برنامج لمهاجمة موقع الكتروني أو إرسال بريد يحتوي على برنامج يعمل تلقائيا.

و تنفرد الجريمة المعلوماتية بعدة خصائص تميزها عن الجريمة التقليدية ومنها طبيعة تلك المعلومات محل الجريمة, حيث أن المعلومات بطبيعتها غير المادية يمكن أن تخضع لأكثر من

نص قانوني وفقا لما إذا كانت في شكل مادي أو غير مادي, وفي الشكل المادي يوجد لها أكثر من نص قانوني يمكن أن يطبق [1].

فقد عالجت المادة (445/أ) من قانون العقوبات الأردني ما يقع من ضرر أو تخريب أو إتلاف لمال الغير حيث نصت على: (كل من الحق باختياره ضرراً بمال غيره المنقول ، يعاقب بناء على شكوى المتضرر بالحبس مدة لا تتجاوز سنة أو بغرامة لا تتجاوز خمسين ديناراً أو بكلتا العقوبتين.

وكذلك نصت المادة (72) من قانون الاتصالات رقم (13) لسنة 1995 على انه:

أ . كل من أقدم قصدا " على تخريب منشآت الاتصالات أو الحق بها ضررا " عن قصد يعاقب بالحبس لمدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين او بغرامة لا تقل على (200) دينار ولا تزيد على (5000) دينار او بكلتا العقوبتين، وتضاعف العقوبة اذا تسبب فعله بتعطيل حركة الاتصالات.

ب. كل من تسبب إهمالا" في تخريب منشآت الاتصالات او الحاق الضرر بها يعاقب بالحبس مدة لا تزيد على ثلاثة أشهر أو بغرامة لا تزيد على(100) دينار أو بكلتا العقوبتين)

و باستقراء نص المادة 445 من قانون العقوبات نجد انه يمكن انطباق نص هذه المادة على إتلاف المال المعلوماتي المادي كإتلاف قرص ممغنط أو لوحة المفاتيح.

---

[1] إبراهيم .خالد ممدوح . مرجع سابق ص88

وقد جاءت المادة (72) من قانون الاتصالات الأردني لتجرم أفعال الإتلاف الخاصة بأدوات الحاسب الآلي وشبكاته التي تؤثر على سير عمل النظام المعلوماتي ومسألة الإتلاف المادي لمنشآت الاتصال, ومثال ذلك قيام احد الأشخاص بقطع كوابل إحدى الشبكات المغلقة .

ونستتج مما سبق انه يمكن انطباق نص المادة (445) من قانون العقوبات، و المادة (72) من قانون الاتصالات على فعل الإتلاف المادي لأنظمة المعلومات والشبكات المرتبطة بها , لكن هذه المواد لا يمكن انطباقها على إتلاف البيانات والبرامج المعنوية (الغير ملموسة) والغير موجودة على دعامة تحتويها, لان المادتين السابقتين عالجتا ما يقع على أنظمة المعلومات من إتلاف مادي دون التطرق إلى تجريم ما يقع من إتلاف للبيانات والبرامج الغير ملموسة والتي جرمتها المادة (4) من قانون جرائم أنظمة المعلومات.

الفرع الأول

الركن المادي في فعل الإدخال

سنبحث صور الركن المادي في فعل الإدخال كما يلي:

يتحقق فعل الإدخال بإضافة معطيات جديدة على الدعامة الالكترونية سواء كانت خالية أم يوجد عليها معطيات, وتلك الجريمة تقع في الغالب بمعرفة المسئول عن القسم المعلوماتي والذي يسند إليه وظائف المعاملات أو المحاسبات لأنه يكون في أفضل وضع يؤهله لارتكاب هذا النمط من التلاعب الغير المشروع [1].

[1] حجازي .عبد الفتاح بيومي . مرجع سابق.ص 378

ومن الصور العملية لإدخال معلومات مصطنعة قيام المسئول المعلوماتي في المنشئة بضم مستخدمين غير موجودين بالفعل أو قيامه بالإبقاء على مستخدمين تركوا الوظيفة بالفعل.

أما إذا أدخل عمداً بطريقة مباشرة أو غير مباشرة بيانات لنظام المعالجة الآلية أو عدل البيانات التي يحتويها أو عالجها أو نقلها فأن ذالك يعد طريقة أو صورة من الإدخال، وتعالج المادة(4) من قانون جرائم أنظمة المعلومات جرائم مهاجمة وتخريب أنظمة المعلومات والشبكة المعلوماتية والمواقع الإلكترونية عن طريق إدخال ونشر واستخدام برنامج بقصد تحقيق أحد النتائج المبينة في البند (ب من المادة 3 من قانون جرائم أنظمة المعلومات)إلا أن هناك فرق بين المادة الثالثة والمادة الرابعة هو أن المادة الرابعة لا تشترط الدخول لنظام بقصد تحقيق إي من تلك النتائج بل يكفي استخدام برنامج عن بعد لهذه الغاية مثل إرسال فيروس عبر البريد الالكتروني أو استخدام برنامج لمهاجمة موقع الكتروني, وهناك أنواع أخرى لمثل تلك البرامج تستطيع سرقة معلومات وإرسالها وتخريب المواقع الاكترونية.

ويتبين من نص المادة الرابعة أن المشرع لم يكتفي بالقصد العام فقط إلا أنه أضاف قصد خاص لارتكاب جريمة الإدخال لأن إدخال ونشر مثل هذه البرامج يجب لكي يكون مجرماً أن يتم بقصد ارتكاب الفعل فمجرد تخزين مثل هذه البرامج أو نشرها بقصد الاستخدام المشروع لا يشكل جرماً.

الفرع الثاني

استخدام برامج خبيثة لإتلاف البيانات أو تعطيل عمل النظام المعلوماتي

ويقصد بالإتلاف المعلوماتي : أن يتم محو البيانات أو المعلومات أو البرامج كلياً أو تدميرها الكترونياً أو أن يتم تشويه المعلومات أو البرامج على نحو فيه إتلاف مما يجعلها غير صالحة للإستعمال[1].

كما أن الإتلاف قد يكون كلياً عند محو وتدمير جميع البيانات والبرامج الموجودة في النظام, وقد يكون جزئياً ويطلق عليه في هذه الحالة (تشويه أو تعييب) ويتمثل في إدخال برامج خبيثة داخل الجهاز تقوم على إنقاص كفائته أو إبطاء حركة الجهاز ذاته [2].

كما أن معظم محاولات اختراق النظم المعلوماتية تتم عن طريق برامج متوفرة على شبكة الإنترنت بحيث يستطيع أي شخص ذو معرفة بسيطة في مجال المعلوماتية أن يقوم بتحميلها واستخدامها بطرق غير مشروعة لشن هجماته على أجهزة الغير متمتعاً بالإمكانيات المتعددة التي تقوم بها هذه البرامج [3].

ويمكن تعريفها بأنها : عبارة عن برامج خبيثة تتسلل إلى البرمجيات بحيث تدخل اليها وتنسخ نفسها على برامج أخرى في الحاسب الآلي [4].

أساليب إتلاف البيانات والمعلومات داخل النظام المعلوماتي:

---

[1] الملط , احمد خليفة ,مرجع سابق ,ص 518 .

[2] سلامة,محمد عبد الله(2006).**جرائم الكمبيوتر و الانترنت**.الاسكندرية:منشأة المعارف.ص152

[3] إبراهيم .خالد ممدوح , مرجع سابق, ص246

[4] الشوابكة,محمد أمين(2009).**جرائم الحاسوب والإنترنت**,ط1.عمان:دار الثقافة.ص238

يحدث إتلاف البيانات والمعلومات الموجودة داخل النظام المعلوماتي بعدة أساليب تتمثل في ثلاثة أنواع كالتالي:

أولا . برامج الفيروس:

والفيروس هو عبارة عن برنامج يصممه الجاني ذو الكفاءة والخبرة في مجال أنظمة المعلومات, ويهدف من خلاله إلى الوصول إلى البرامج والنظام المعلوماتي للغير, ويكون الفيروس عبارة عن مجموعة من التعليمات التي تتكاثر بمعدل سريع جدا لدرجة أنها تصيب النظام المعلوماتي بالشلل التام, ويتميز الفيروس بعدة خصائص كالقدرة على الاختفاء لحظة وصوله إلى جهاز الضحية وأيضاً القدرة على الانتشار بين أجهزة الحاسوب إذا كانت متصلة ضمن الشبكة بالإضافة إلى قدرته على الدخول و التسلل داخل النظام المعلوماتي, ويسفر عن ذلك تدمير البرامج والمعلومات وتعوق الاتصال وتشوه البيانات بل وتضلل المستخدم احياناً ببيانات خاطئه ومن الأمثلة على هذه الفيروسات فيروس ميليسا وفيروس الحب [1].

ثانياً. برامج الدودة:

يقوم نظام عمل هذه البرامج بالبحث عن أي فجوة في نظام التشغيل للدخول منها, وتتميز برامج الدودة بقدرتها على التنقل من جهاز حاسوب إلى آخر أو عن طريق الشبكة إذا كانت هذه الأجهزة متصلة ببعضها البعض, كما أنها تتكاثر إثناء عملية انتقالها بإنتاج نسخ تلقائية عنها, ومن الأضرار الناتجة عنها خفض كفاءة الشبكة بإشغال أي حيز من سعة الشبكة كما تؤدي إلى تخريب و إتلاف البيانات والملفات والبرامج الموجودة داخل النظام المعلوماتي.[2]

---

[1] زين الدين, بلال أمين, مرجع سابق ,ص 372

[2] الشوابكة,محمد أمين,مرجع سابق,ص240

ثالثاً. برامج القنبلة المعلوماتية:

وتنقسم إلى قسمين:

1. القنبلة المنطقية :

وهي عبارة عن برامج صغيرة أو أجزاء من برامج ينفذ في لحظه محددة أو لفتره زمنية منتظمة فهي تظل ساكنه وبدون فعالية وبالتالي قد تكون غير مكتشفه لمده طويلة من الزمن, كما يتم إدخالها بطرق فنية غير مشروعة مع برامج أخرى بحيث تعمل على مبدأ التوقيت فتحدث إتلافاً وتخريب في البيانات والمعلومات والبرامج عند تطبيق أمر معين في الحاسب الآلي حيث يكون الهدف منها تدمير و تغيير البرامج ومعلومات النظام في لحظه معينة أو فترة زمنية محددة [1].

2.القنبلة الزمنية :

وسميت كذلك لأنها تنشط وتبدأ نشاطاتها التدميرية عند حدوث واقعة محددة أو في تاريخ يحدد سلفاً, فهي تثير حدثا في لحظه زمنية محددة بالساعة واليوم والسنة ويتم إدخالها ببرامج وتنفذ في جزء من الثانية وفقا للتحديد أللازم [2].

ومن الأمثلة الواقعية عليها قيام احد الموظفين بإحدى الشركات الكبرى بولاية تكساس الأمريكية عام 1985 بوضع قنبلة زمنية في شبكة المعلومات الخاصة بهذه الشركة بعد

---

[1] سلامة,محمد عبد الله,مرجع سابق,ص153

[2] الملط ,احمد خليفة , مرجع سابق ,ص195

الاستغناء عن خدماته وبدافع الانتقام حيث انفجرت بعد مضي ستة أشهر من رحيله وترتب على ذلك محو أكثر من 168 ألف سجل من عمولة المبيعات الخاصة بهذه الشركة [1].

المبحث الثاني

جريمة الحصول على معلومات تتعلق بالغير

أدت الثورة الرقمية إلى إمكانية إجراء مبادلات للبيانات والمعلومات عن طريق إرسالها عبر شبكات الإتصال العالمية والمحلية, وهذا ما أتاح للمجرم المعلوماتي ممارسة نشاطاته الإجرامية من أجل تحقيق غايات شخصية متعلقة بذات المجرم, بحيث يتمكن الجاني من التقاط البيانات المخزنة والمتبادلة عبر النظام المعلوماتي كمعرفة الأرقام الخاصة ببطاقة الائتمان

[1] سلامة,محمد عبد الله,مرجع سابق,ص154

والاعتراض على الرسائل المنقولة عبر شبكات الإتصال أو التصنت على ما هو مرسل عن طريق شبكات الاتصال[1].

وسوف نخصص هذا المبحث للحديث عن جريمة الإلتقاط غير المشروع للبيانات وفق ما جاءت به المادة (5) من قانون جرائم أنظمة المعلومات رقم (30) لسنة (2010) في مطلب أول ومن ثم نتناول جرائم إساءة استخدام بطاقات الائتمان في مطلب ثاني وفق ما جاءت به المادة (6) من نفس القانون, كما سوف نتطرق إلى بيان الركن المادي و المعنوي لهذه الجرائم و موقف المشرع الأردني منها.

وعليه ارتأيت إلى تقسيم هذا المبحث كالتالي:

المطلب الاول : جريمة الإلتقاط غير المشروع للبيانات.

المطلب الثاني :جريمة إساءة استعمال بطاقات الائتمان.

المطلب الأول

جريمة الإلتقاط غير المشروع للبيانات

جرمت المادة (5) من قانون جرائم أنظمة المعلومات المؤقت لسنة 2010 إعمال الالتقاط والاعتراض والتصنت, حيث نصت المادة الخامسة منه على انه: (كل من قام قصدا دون سبب مشروع بالتقاط أو باعتراض أو بالتصنت على ما هو مرسل عن طريق الشبكة المعلوماتية

[1] الشوابكة,محمد أمين,مرجع سابق,ص166

أو أي نظام معلومات يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا هاتين العقوبتين).

و كذلك نصت المادة (356) من قانون العقوبات الأردني على انه:

(1- يعاقب بالحبس من شهر إلى سنة كل شخص ملحق بمصلحة البرق والبريد يسيء استعمال وظيفته هذه بأن يطلع على رسالة مظروف أو يتلف أو يختلس إحدى الرسائل أو يفضي بمضمونها إلى غير المرسل إليه.

2- ويعاقب بالحبس مدة ستة أشهر أو بالغرامة حتى عشرين دينارا من كان ملحقا بمصلحة الهاتف وأفشى مخابرة هاتفية اطلع عليها بحكم وظيفته أو عمله).

كما نصت المادة (357) من قانون العقوبات الأردني على انه:

(كل شخص يتلف أو يفض قصدا رسالة أو برقية غير مرسلة إليه يعاقب بغرامة لا تتجاوز الخمسة دنانير).

إذا كانت نصوص هذه المواد من قانون العقوبات تتحدث عن هذه الصورة ولكن بصورتها سلوكاً تقليدياً مادياً قوامه فض الرسائل وتبيان محتواها أو كشف محادثات هاتفية والإطلاع على محتواها, فإن مادية هذه السلوكيات تقف بالنص موقف العاجز عن مد نطاق التجريم إلى حد شمول النموذج المستحدث لهذه الجريمة فلا يمكن انطباق هذه النصوص على الرسائل والمحادثات الإلكترونية .

وقد جرم المشرع في قانون الاتصالات سلوكيات ذات صله باعتراض الاتصال التقني لأنظمة المعلومات فقد نصت المادة (76) من قانون الاتصالات رقم 13 لسنة 1955

وتعديلاته على أنه: (كل من اعترض او اعاق او حور او شطب محتويات رسالة بواسطة شبكات الاتصالات او شجع غيره على القيام بهذا العمل يعاقب بالحبس مدة لا تقل على شهر ولا تزيد على ستة اشهر او بغرامة لا تزيد على (200) دينار او بكلتا العقوبتين).

ويلاحظ على هذا النص انه أحاط بكافة صور اعتراض الاتصالات التقنية لأنظمة المعلومات بل تعدى ذلك إلى صور الاعتداء على محتويات الرسالة ،كما أنه عنى هذا النوع الجديد من الإجرام الالكتروني, كذالك انه يعاقب بذات العقوبة على مجرد التشجيع على إتيان الفعل وهو توسيع لنطاق التجريم وإدخال صريح للتحريض في نطاق التجريم, إلا انه يؤخذ عليه عدم إتيانه بعقوبة جزائية رادعة توافق بين خطورة الفاعل الاجرمية وعظم الآثار الناتجة عن فعلة ومدى الإضرار التي يمكن أن تصيب المجني عليه أو تلك التي يمكن أن تلحق نظام المعالجة الإلية للبيانات والمعلومات.

ومن الواضح أن نص المادة (5) من قانون جرائم أنظمة المعلومات شبيه بنص المادة (76) من قانون الاتصالات رقم (13) لسنة1995 فقد جرمت هذه المادة أيضاً أفعال الالتقاط غير المشروع للبيانات وأفعال الاعتراض و التصنت على المراسلات الالكترونية.

ويثور التساؤل هنا عن مدى انطباق أي من المادتين على ما يقع من اعتراض للرسائل المنقولة عن طريق أنظمة المعلومات و شبكات الاتصال؟

لقد تم تجريم الالتقاط والاعتراض والتصنت على ما هو مرسل عن طريق الشبكة المعلوماتية أو نظام معلومات آخر في قانون جرائم أنظمة المعلومات لوجود فرق ما بين شبكة الاتصالات العامة والخاصة وبين شبكة المعلومات، فكل من شبكة الاتصالات العامة (والتي تحتاج لترخيص) وشبكة الاتصالات الخاصة تم تنظيمها بموجب قانون الاتصالات على اعتبار أن

كلا الشبكتين يتم إنشائهما وربطهما وفقا لأحكام قانون الاتصالات، وعلى وجه الخصوص، فإن شبكة الاتصالات الخاصة بموجب قانون الاتصالات هي منظومة اتصالات تشغل لمصلحة شخص واحد أو مجموعة واحدة من الأشخاص تجمعهم ملكية مشتركة لخدمة حاجاتهم الخاصة، وهذا لا ينطبق على شبكة المعلومات التي قد تربط بين جهات متعددة داخل المملكة وخارجها عبر الانترنت، كما لا تسري أحكام شبكة الاتصالات العامة بحق شبكة المعلومات كون شبكة الاتصالات العامة بموجب قانون الاتصالات تحتاج ترخيصا بينما شبكة المعلومات عبر الانترنت وإن كانت تحتاج المرور بشبكة اتصالات عامة أو خاصة إلا أنها قد تكون مربوطة بشبكة اتصالات أخرى خارج المملكة لا تحتاج ترخيص ولا تسري عليها أحكام القانون الأردني[1]، والمثال على ذلك مواقع المحادثة عبر الانترنت التي تقدم خدمات الربط بين أكثر من مستفيد، فهي غير مرخصة في الأردن لتقديم تلك الخدمة على الرغم من أنها تؤدي خدمة شبكة اتصالات عامة وتربط بين أشخاص مقيمين داخل المملكة وتربط بينهم وبين أشخاص غير مقيمين بها، وبالتالي فإن شبكة المعلومات قد تحتوي على أكثر من شبكة اتصالات خاصة وعامة لا ينطبق على بعضها أو معظمها قانون الاتصالات.

ولبيان الركن المادي لهذه الجريمة سنقسم هذا المطلب إلى فرعين كالتالي:

الفرع الأول

جريمة إعتراض الرسائل المنقولة عبر شبكة الانترنت

[1] المذكرة الايضاحية لقانون جرائم أنظمة المعلومات رقم (30) لسنة (2010) ,ص4

عرف الاعتراض بأنه : التصنت أو نقل البيانات التي تتم داخل جهاز الحاسب أو التي تتم عبر جهازين عن بعد عبر الشبكات المعلوماتية المختلفة أو بترجمة الإنبعاثات الكهرومغناطيسية الصادرة من الحاسب أو التي تتم عبر الأجهزة اللاسلكية وذلك عن طريق أي من الوسائل الفنية الغير علنية[1].

حيث يعتمد هذا السلوك على اختراق الجاني لأنظمة المعلومات, لكن محل الجريمة هنا ليس النظام بذاته بل الرسائل المنقولة والمتبادلة بين هذه الأنظمة المتصلة فيما بينها عن طريق الشبكات المحلية المغلقة أو الشبكات العالمية المفتوحة, كما و يتمثل اعتراض الرسائل في صورة منع وصولها إلى جهة إرسالها ويقتضي هذا السلوك تحقق فعل الاختراق ثم تحقق منع وصول الرسالة إلى الجهة المحددة من قبل المرسل سواءً أمكن معرفة محتوى الرسالة أو لم يمكن فهدف الجاني يكمن في منع وصول الرسالة إلى الجهة المقصودة[2].

الفرع الثاني

جريمة التصنت على المراسلات الإلكترونية

يتمثل هذا الأسلوب في قيام الجاني باستخدام برامج تتيح له الإطلاع على المعلومات الخاصة بمستخدمي شبكات الاتصال المحلية أو العالمية, وتتباين خطورة التجسس بحسب أهمية

---

[1] زين الدين, بلال أمين,مرجع سابق, ص 306
[2] الزعبي,جلال و المنعسةوأحمد,مرجع سابق,ص253

المعلومات والبيانات الملتقطة فقد تكون معلومات سرية تجارية أو معلومات عسكرية أو معلومات خاصة ببطاقات الائتمان أو معلومات شخصية أو غير ذلك من المعلومات[1].

كذلك فقد تتنوع الأساليب الفنية في التصنت على المراسلات , كدس وحدات ناقلة للبيانات داخل أجهزة الحاسب الآلي وتوصيلها كهربائياً بشكل خفي أو أخفاء برامج خبيثة في البرامج التطبيقية الموجودة على النظام, بحيث تسمح بالوصول عن بعد إلى قاعدة البيانات لقراءتها أو تسجيلها أو نقلها دون أن يشعر بذلك أحد, كما يمكن استخدام هوائيات متصلة بحاسب خاص لالتقاط وتسجيل الموجات الكهرومغناطيسية التي تنبعث من الحاسب, كما يمكن استخدام أسلوب الأبواب الخفية (المصيدة) الذي يعتمد على البحث في الثغرات الموجودة في البرامج من الدخول من خلالها إلى النظام والاطلاع على البيانات المخزنة بداخله.[2]

كذلك قد يتم التصنت من خلال أجهزة متطورة تقوم بالتقاط الذبذبات والترددات المختلفة والقيام بتحليلها وفك رموزها أو شيفرتها, وقد يكون عن طريق الحاسبات الآلية من خلال استراق السمع عبر البريد الإلكتروني وما يتم عبر شبكة الانترنت من محادثات صوتية أو أثناء انتقالها عبر الشبكة من جهاز لآخر فيتمكن الجاني من سماع هذه المحادثات والإطلاع على المعلومات مستعيناً بهذه الأدوات أو البرامج الغير مشروعة[3], و تجدر الإشارة هنا إلى أن هذه الجرائم لا تكون إلا مقصودة وهذا ما أشارت له المادة (5) من قانون جرائم أنظمة المعلومات بقولها (كل من قام قصداً) بحيث لا يتصور وقوعها بخطأ أو إهمال.

---
[1] الشوابكة,محمد أمين,مرجع سابق,ص166
[2] سلامة,محمد عبد الله ,مرجع سابق, ص148
[3] زين الدين,بلال أمين,مرجع سابق,ص288

المطلب الثاني

جريمة إساءة استعمال بطاقات الائتمان

يمكن تعريف بطاقة الائتمان بأنها: أداة دفع وسحب نقدي يصدرها مصرف تجاري أو مؤسسة مالية تُمكن حاملها من شراء السلع والخدمات ممن يعتمد المستند دون دفع ثمن حالاً لتضمنه التزام المصدر بالدفع ومنها ما يمكن من سحب النقود من المصارف.[1]

كما ويمكن استخدام هذه البطاقة في عملية شراء السلع والخدمات عبر شبكة الانترنت عن طريق تصريح تقني بخصم القيمة على حساب بطاقة الدفع الالكتروني الخاصة به, وقد أتاحت الثورة الرقمية لقراصنة المعلوماتية استغلال هذه البطاقة للحصول على الأموال بطريقة غير

[1] موسى.مصطفى محمد(2005),**اساليب اجرامية بالتقنية الرقمية** ,مصر:دار الكتب القانونية,ص161

مشروعة وذلك بتخليق أرقام بطاقات بنك معين بتزويد الحاسوب بالرقم الخاص بالبنك مصدر البطاقة علاوة على إمكانية التقاط هذه الأرقام عبر شبكة الإنترنت واستخدامها بطرق غير مشروعة في عملية الشراء عبر الإنترنت وخصم قيمة تلك السلع من حساب العملاء الشرعيين لهذه البطاقات.[1]

وقد عالج المشرع الأردني مسألة الاعتداء على بيانات ومعلومات البطاقات الائتمانية والتي تقع باستخدام النظم المعلوماتية وشبكة الانترنت خاصة, حيث نصت المادة (6) من قانون جرائم أنظمة المعلومات المؤقت على انه :

(أ. كل من حصل قصدا دون تصريح عن طريق الشبكة المعلوماتية او أي نظام معلومات على بيانات او معلومات تتعلق ببطاقات الائتمان او بالبيانات او المعلومات التي تستخدم في تنفيذ المعاملات المالية او المصرفية الالكترونية يعاقب بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنتين او بغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (2000) الفي دينار أو بكلتا هاتين العقوبتين).

ب. كل من استخدم عن طريق الشبكة المعلوماتية او أي نظام معلومات قصدا دون سبب مشروع بيانات او معلومات تتعلق ببطاقات الائتمان او بالبيانات او المعلومات التي تستخدم في تنفيذ المعاملات المالية او المصرفية الالكترونية للحصول لنفسه او لغيره على بيانات او معلومات او اموال او خدمات تخص الاخرين يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن (1000) الف دينار ولا تزيد على (5000) خمسة الاف دينار).

[1] الشوابكة ,محمد أمين ,مرجع سابق, ص194.

ورغبة من المشرع الأردني في الحفاظ على استقرار المعاملات المالية الالكترونية وتشجيعها فقد تم وضع هذا النص الذي يجرم الحصول على تلك المعلومات عن طريق الشبكة المعلوماتية أو أي نظام معلومات, كما هو الحال في تعقب المعاملات المالية أو قواعد البيانات الخاصة ببطاقات الائتمان والحصول منها على رموز ومعلومات استخدامها، ولا يشترط قيام الفاعل باستخدام هذه المعلومات لتطبيق العقوبة بحقه فمجرد الحصول على تلك المعلومات قصدا دون سبب مشروع يعد جريمة قائمة بذاتها تستوجب العقوبة كما هو الحال في سرقة بطاقة الائتمان، فالمعلومات الخاصة ببطاقة الائتمان لا تقل أهمية عن البطاقة ذاتها ويستوجب حمايتها لمنح الثقة بالمعاملات المالية الالكترونية وحماية للحقوق المالية لمالكيها[1].

ويرى الباحث أن المال المعلوماتي يدخل ضمن تعريف المال الذي أورده المشرع في المواد

(53و54) من القانون المدني رقم 43 لسنة 1976 حيث نصت هذه المواد على ان:

المادة 53- (المال هو كل عين او حق له قيمة مادية في التعامل).

المادة 54- (كل شيء يمكن حيازته ماديا او معنويا والانتفاع به انتفاعا مشروعا ولا يخرج عن التعامل بطبيعته او بحكم القانون يصح ان يكون محلا للحقوق المالية).

وباستقراء نصوص المواد السابقة نجد أن المال المعلوماتي له قيمة مادية في التعامل ومثال ذلك برامج وتطبيقات الحاسوب المعدة للبيع كذلك فإن المال المعلوماتي يمكن حيازته معنوياً ومادياً ولا يخرج عن التعامل بطبيعته فيمكن مثلا حيازة المعاملات المالية والبيانات والبرامج على دعامة مادية كالقرص الصلب والقرص المضغوط بحث تصبح هذه الدعامة ذات قيمة مالية بما تحتوية.

[1] المذكرة الايضاحية لقانون جرائم أنظمة المعلومات رقم (30) لسنة (2010) , ص5

كما و يمكن أن تنطبق بعض نصوص قانون العقوبات الأردني على ما يقع من اعتداء مادي على بطاقات الائتمان في حال كان هذا الاعتداء ينصب على جسم البطاقة (المادي) وليس المعلومات والبيانات التي تحتويها هذه البطاقة, فيتصور وقوع جريمة السرقة المنصوص عليها في المادة (399) عند قيام الجاني بأخذ البطاقة من صاحبها الشرعي دون رضاه كما و يمكن وقوع جريمة الاحتيال الواردة في المادة (417) من قانون العقوبات في حال قيام صاحب البطاقة الشرعي أو الغير باستعمال طرق احتياله بإيهام المجني عليه بوجود ائتمان وهمي في حال كانت هذه البطاقة ملغية أو منتهية الصلاحية, كما ويتصور وقوع جريمة إساءة الائتمان عندما يرفض صاحب البطاقة إرجاعها إلى الجهة مصدرة البطاقة –البنك– في حال انتهاء المدة المتفق عليها في عقد عارية الاستعمال .

أما إذا ارتكبت هذه الجرائم – السرقة, الاحتيال, إساءة الائتمان– باستخدام النظام المعلوماتي والشبكة المعلوماتية فإن المادة (6) من قانون جرائم أنظمة المعلومات هي الواجبة التطبيق في هذه الحالة.

وغاية المشرع من تجريم الحصول على البيانات والمعلومات خاصة تلك التي تتعلق ببطاقات الائتمان, وذلك لكونها تعد الأكثر انتشارا من بين البطاقات المالية عموماً والتي يستخدمها الأفراد في الحصول على تسهيل ائتماني من مصدر هذه البطاقة ويتم من خلالها القيام بالوفاء والإيداع ولذلك سميت هذه البطاقات بالبطاقات الائتمانية؛ لاشتمالها على القرض، والقرض من صور الائتمان؛ لأن الائتمان مبادلة مال حاضر بمؤجل، والقرض كذلك [1].

ويمكن تصور الركن المادي لجريمة إساءة استعمال بطاقات الائتمان كما يلي:

[1] الحسيناوي,علي جبار(2009).**جرائم الحاسوب والانترنت**.عمان:دار اليازوري.ص85

الفرع الأول

إساءة استخدام البيانات من قبل حاملها الشرعي

تكمن إساءة استخدام بيانات بطاقة الائتمان من قبل صاحبها في صورتين, إما باستخدام بيانات البطاقة الائتمانية أثناء صلاحيته وإما باستخدام بيانات البطاقة الائتمانية بعد انتهاء مدة صلاحيتها أو إلغائها وذلك كالتالي:

أولاً. إساءة استخدام بيانات البطاقة الائتمانية أثناء مدة صلاحيتها:

وتتصور هذه الحالة عندما يقوم العميل بتقديم البطاقة إلى التاجر رغم علمه أن رصيده بالبنك غير كافي لتغطية هذه المبالغ وأنه استنفذ حدود الائتمان الممنوح له, حيث يقوم البائع بحسن نية بتسجيل عملية البيع وإعداد الفواتير لتقديمها للجهة مصدرة البطاقة وقد أختلف الفقهاء حول تحديد الوصف القانوني لهذه الأفعال فمنهم من تصور وقوع جريمة السرقة وحجتهم بذلك أن العميل بقيامه بهذا التصرف يقوم بأخذ مال الغير دون رضاه بطريقة غير مباشرة وبالتطبيق وبعد تمام عملية البيع باستخدام البطاقة فارغة الرصيد فإن هذه العملية تخلو من فعل أخذ النقود المودعة لدى البنك, كما أن تسليم المشتريات يتم بطريقة رضائيه مما ينفي فعل الأخذ غير رضائي وبانتفاء العناصر الأساسية لجريمة السرقة يترتب عليه انتفاء هذا الوصف عن هذه التصرفات[1].

ومنهم من تصور وقوع فعل الاحتيال وحجتهم بذلك أن تقديم العميل للبطاقة الائتمانية إلى التاجر وهو يعلم بعدم وجود رصيد كافي وبهذه الحالة يكون قد أوهم التاجر من خلال الجهاز

---

[1] الزعبي,جلال و المناعسة,أحمد ,مرجع سابق,ص 202

الخاص بهذه البطاقة انه يملك الحق باستخدام هذه البطاقة بحدود قيمة مشترياته, وقد عارض أغلب الفكر باعتبار صاحب البطاقة المتجاوز للرصيد يعد محتالاً واستندوا في ذلك أن الجهاز مبرمج بواسطة البنك لأجازة عملية السحب أو رفضها فإذا سمح الجهاز بتسليم النقود فلا تتوافر الطرق الاحتيالية لحمل هذا الجهاز على التسليم أو إقناعه بوجود ائتمان وهمي [1].

وقد أنكر الفقه أيضا انطباق وصف إساءة الائتمان على هذا الفعل حتى مع التسليم بأن البطاقة بمقتضى العقد تكون ملكاً للجهة المصدرة لها, إلا أن استيلاء العميل على مبالغ نتيجة استخدامه للبطاقة وتجاوزه للحد الأعلى المسموح به فإن هذا الفعل لا يعدو مجرد إخلال بالالتزام التعاقدي.

ويري الباحث انه لا يمكن انطباق وصف السرقة أو الاحتيال أو إساءة الائتمان على هذا الفعل ذلك لأن بطاقات الائتمان وأجهزة السحب الحديثة مزوده ببرامج وتعليمات فنية تمنع عملية سحب النقود بعد انتهاء مدة صلاحيتها أو تجاوز حدود سقف الائتمان, وعلى فرض تمت عملية السحب بعد انتهاء صلاحية البطاقة فإن الفعل لا يخرج عن نطاق الاخلال بالالتزام التعاقدي ما بين المستفيد و مصدر البطاقه ذلك لان كل عملية سحب تسجل الكترونيا لدى مصدر البطاقة وعليه يتم الرجوع الى شروط العقد المبرم ما بين الطرفين .

ثانياً.إساءة استخدام بطاقة الائتمان بعد انتهاء مدة صلاحيتها أو إلغاؤها:

إذا قام العميل باستعمال بطاقة الائتمان بعد إلغائها من قبل البنك فإن فعله يشكل جريمة احتيال, ويكون هذا الاحتيال في إيهام جهاز التوزيع الآلي للنقود التابع للبنك بوجود ائتمان على خلاف الحقيقة, ويتحقق الاحتيال في نطاق شبكة الانترنت بملء البيانات الخاصة ببطاقة

---

[1] الشوابكة .محمد أمين , مرجع سابق ص195

الائتمان على النموذج الالكتروني بهدف الإيهام بوجود ائتمان بنكي صالح المدة, إذ أن إلغاء البطاقة يخلع عنها قيمتها كأداة ائتمان بالإضافة إلى تحقق عنصر التسليم حين قيام التاجر بتسليم المشتريات إلى صاحب البطاقة الملغاة , إلا أن التكنولوجيا الحديثة قد واجهت مثل هذه التصرفات وذلك بتزويد الآلة الالكترونية ببرامج حماية تجعلها تتفادى هذا الغرض من تلقاء نفسها[1] .

ومن المعلوم أن العلاقة ما بين العميل وما بين مصدر البطاقة هي علاقه تعاقديه تكون غالباً على أساس عقد عارية الاستعمال, بحيث يعهد العميل إلى استعمالها وإرجاعها وفق ما هو مدون في العقد وفي حال امتناع العميل عن رد البطاقة فإن فعله يشكل اختلاس تقوم به جريمة خيانة الامانه, بحيث تعتبر تبديداً للشيء الذي تم تسلمه على سبيل عارية الاستعمال ويكفي لتوافر الاختلاس أن ينكر حامل البطاقة وجودها في حيازته[2].

الفرع الثاني

إساءة استخدام بطاقة الائتمان بواسطة الغير

يمتاز استخدام بطاقة الائتمان بالطابع الشخصي بحيث تخول صاحبها فقط من استخدام هذه البطاقة كما أن الطبيعة الخاصة للبطاقة الائتمانية تفرض على حاملها ألمحافظه عليها والمحافظة على الرقم السري الخاص بها بصورة تمنع الغير من استخدامها, كذلك تفرض التزامات على صاحب البطاقة بأن لا يضع الرقم السري بصحبتها وان يقوم بإبلاغ البنك حال

[1] زين الدين,بلال أمين,مرجع سابق,ص147
[2] الشوابكة,محمد أمين,مرجع سابق,ص197

فقدانها, وقد شهد الواقع العملي عدة صور لإساءة استخدام هذه البطاقة من قبل الغير كالحالات التي تتعرض لها البطاقة للسرقة أو الفقدان أو حالة سرقة كلمة السر من خلال شبكة الانترنت واستخدامها بطرق غير مشروعه في سحب النقود أو تخليق أرقام بطاقات ائتمانية أو استغلال الأرقام الخاصة بالغير واستخدامها بصورة غير مشروعه [1].

ومن الأمثله الواقعيه على هذه الجريمة قيام ثمانية أمريكيين في نهب 45 مليون دولار من بنكين خليجيين والبنكان هما بنك مسقط العماني، الذي كان أكبر الخاسرين، وبنك رأس الخيمة الإماراتي، والثغرة التي تم استغلالها من قبل العصابة، كانت شركة هندية تزود كليهما ببطاقات الائتمان, وفقا للتحقيقات فإنّ العصابة نجحت في اختراق معلومات الشركة الهندية، ومن ثمّ قاموا بإزالة سقف السحوبات من بطاقات الائتمان. وتم سحب نحو 40 مليون دولار من بنك مسقط ونحو خمسة ملايين من بنك رأس الخيمة.[2]

ويثور التساؤل في هذا الصدد حول التكييف القانوني في استخدام بيانات بطاقة الائتمان من قبل الغير على شبكة الانترنت وللبحث في هذا التساؤل سنتطرق إلى حالتين و هما:

أولاً. حالة سرقة بيانات بطاقات الائتمان:

يأخذ البنك التزام من العميل بأن لا يعطي الرقم السري لأي شخص حتى لا يقع ضحية استعمال غير مشروع لها من قبل الغير, ولذلك فإن العميل وحده يكون مسئولاً عن الإدلاء بأرقام بطاقة الائتمان عبر شبكة الإنترنت وعن تعرضها للاحتيال سواءً بفعل التجسس أو الخداع .

---

[1] الزعبي,جلال و المناعسة,أجمدومرجع سابق,ص 216

[2] بوابة الاردن,2013,قرصنه مالية تنهب بنكين خليجيين,متاح:
http://www.jordan1one.com/news/2013/05/12/17689.html

وإذا كانت طبيعة التجارة الإلكترونية والشراء من الإنترنت يتطلب تعبئة النموذج الخاص ببطاقة الائتمان ومنها الرقم السري الخاص بها ، فهل يعتبر صاحب البطاقة الشرعي مسئولاً في حال فقدان أو سرقة الرقم السري للبطاقة من قبل الغير ؟

مما لا شك فيه أن مسؤولية الحامل الشرعي للبطاقة تنتفي من اللحظة التي يتم فيها إبلاغ البنك عن سرقة البيانات الخاصة لبطاقة الائتمان ، فإذا لم يقم العميل بذلك فلا يعد البنك مسئولاً عن المبالغ التي قام الجاني بالاستيلاء عليها، ويتوجب على البنك (مصدر البطاقة) أن يقوم بإيقاف البطاقة وحجب التعامل فيها[1]،

وقد ذهبت أحكام بعض المحاكم الفرنسية إلا أن سرقة الأرقام والبيانات السرية الخاصة ببطاقة الائتمان واستخدامها بصورة غير مشروعة من قبل الغير تعتبر احتيالاً من جانب الجاني, كما واتجهت بعض الآراء الفقهية إلى مساندة هذه الأحكام بحجة أن إدعاء الجاني بوجود ائتمان على خلاف الحقيقة وانتحال شخصية صاحب البطاقة الأصلي والتصرف بها تصرف المالك يشكل جريمة إحتيال[2] .

ثانياً. حالة استخدام بيانات بطاقة ائتمان مزورة :

عرفت المادة (260) من قانون العقوبات التزوير بأنه (هو تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك او مخطوط يحتج بهما نجم او يمكن أن ينجم عنه ضرر مادي او معنوي او اجتماعي).

---

[1] الشوابكة .محمد أمين , مرجع سابق ص200

[2] زين الدين,بلال أمين,مرجع سابق,ص149

وبالنظر إلى المحررات في نطاق المعلوماتية من بيانات ومستندات معلوماتية، نجد بأنها باتت ضرورة ملحة في عصرنا الحالي لا سيما بعد حلول الحاسب الآلي والمحررات الإلكترونية محل الأوراق في كافة المجالات الحياتية [1].

ويعد التزوير من أخطر طرق الغش في مجال المعالجة الآلية للبيانات على شبكة الإنترنت, ويتمثل تزوير بطاقات الائتمان عبر شبكة الإنترنت بصورة تخليق أرقام بطاقات ائتمان خاصة ببنك معين من خلال تزويد الحاسب بالرقم الخاص للبنك مصدر البطاقة بواسطة برامج تشغل خاصة, كذلك فإن تخليق بيانات بطاقة الائتمان الخاصة بالغير تشكل تعدد الجرائم، حيث يمكن أن ينطبق عليها وصف تزوير واستعمال المزور ويمكن أن ينطبق عليها وصف الاحتيال[2].

الفصل الثالث

الجرائم الخاصة بالإعمال المنافية للآداب العامة

لقد أتاحت التكنولوجيا الحديثة والمتعلقة بالحاسب الآلي والإنترنت آفاقاً أكبر وأوسع للتجارة المثيرة للجنس غير المشروع, حيث أن جهاز الحاسب الآلي وحده دون النظر إلى شبكة الانترنت يشكل جهاز عرض للمواد الإباحية المخلة بالآداب العامة , وبالنظر إلى شبكة الانترنت العالمية فإن تبادل المعلومات على اختلاف أشكالها المكتوبة والمصورة والحية المباشرة قدمت وأتاحت بيئة ملائمة ساهمت في زيادة نسبة الجرائم المثيرة للجنس غير المشروع واستخدامها لأغراض متنوعة , وتكمن الخطورة في محتوى المواد التي تبث عبر

---

[1] سلامة,محمد عبد الله ,مرجع سابق, ص177

[2] الشوابكة .محمد أمين , مرجع سابق ص201

الانترنت والتي تهدف إلى استغلال الأطفال جنسياً والدعوى إلى هدر وإفساد الأخلاق والترويج للدعارة , فشبكة الانترنت هي الزائر دون مقدمات وعلى قدر ايجابياته قد يؤدي في حال انعدام الرقابة على مستخدميه إلى آثار مدمرة وخطيرة خاصة على الأطفال[1].

تقسيم :

سنعمل علي تقسيم هذا الفصل إلي مبحثين سيخصص المبحث الأول للحديث عن المادة (8) من قانون جرائم أنظمة المعلومات رقم (30) لسنة 2010 التي تهدف إلى تشديد إجراءات حماية الأطفال والأحداث من الاستغلال الجنسي عبر الشبكة المعلوماتية, كما سنتناول في المبحث الثاني جرائم الترويج للدعارة والفجور باستخدام أنظمة المعلومات التي نصت عليها المادة (9) من نفس القانون .

المبحث الأول

جرائم الإستغلال الجنسي للأطفال

لا شك بان هناك خطر حقيقي ناجم عن نشر وعرض الصور والمواد الخلاعية عبر شبكة الانترنت باستخدام التقنية الرقمية, مما أدى بالنتيجة إلى الإخلال بالآداب والأخلاق العامة وإلى ظهور تجارة بشعه من نوع جديد وهي تجارة الجنس الخاص بالأطفال, وهي لا تنحصر في حرمان الطفل من أبسط حقوقه ولكنها تعتدي على براءته بصورة سلبية, وهي مسألة متوارثة من عهود سحيقه ولكنها كانت غير ظاهرة على السطح كما هو حالياً فقد تطورت وازدادت وعرف عنها نتيجة الإعلام المفتوح, حيث أنها تمر بحلقه دائرية بمسميات تلاءم كل

[1] حجازي.عبد الفتاح بيومي(2007),الأحداث والإنترنت,مصر:دار الكتب القانونية.ص8

زمان ومكان, فإذا كانت تسمى فيما سبق بتجارة الرق على اختلاف أعمار الرقيق آنذاك فهي تعود اليوم بمسمى تجارة البغاء للأطفال والنساء عبر الانترنت.[1]

وسوف نتناول في هذا المبحث ما جاءت به المادة (8) من قانون جرائم أنظمة المعلومات حول جرائم الاستغلال الجنسي للأطفال عبر شبكة الانترنت وذلك في مطلب أول كما سنبين موقف المشرع الأردني في مطلب ثاني كالتالي:

المطلب الأول: جرائم الاستغلال الجنسي للأطفال عبر الانترنت.

المطلب الثاني: موقف المشرع الأردني من جرائم الاستغلال الجنسي للأطفال.

المطلب الأول

جرائم الاستغلال الجنسي للأطفال عبر الانترنت

لقد وفرت شبكة الانترنت العالمية ساحة كبيرة تستطيع استيعاب أعداد هائلة من المستخدمين وبالتالي سمحت بممارسة جميع أنواع الإجرام الممكنة ومن بينها جرائم الاستغلال الجنسي للأطفال عبر شبكة الانترنت والتي تكمن ماهيتها في نشر مواد إباحية كنشر صور مخلة بالآداب والأخلاق العامة والموجهة إلى شريحة كبيرة من المستخدمين, ومن هنا تبرز الحاجة لحماية الأطفال من أن يكونوا عرضه للمواد الخلاعيه أو أن يكونوا محلاً لها مما يؤدي إلى حدوث أضرار مادية ومعنوية للأطفال, كذلك فإن تصوير الأطفال بأوضاع جنسية مخلة

---

[1] الحمود,وضاح محمود,والمجالي,نشأت مفضي(2005). **جرائم الإنترنت**.عمان:دار المنار للنشر والتوزيع.ص61

بالآداب قد تقع على أطفال حقيقيين أو قد تقع على أطفال افتراضيين و هو ما يسمى بالصور الزائفة كتركيب صور أطفال على أجساد عارية مما يشكل اعتداء على الطفولة.[1]

وقد ظهرت الأخطار المحتملة ضد الأطفال على شبكة الانترنت نتيجة مخاوف رئيسية وهي:

1. إمكانية وصول الأطفال بسهولة إلى مواقع تحتوي مواد إباحية تنظم دعارة الأطفال عبر شبكة الانترنت وتعتبر محركات البحث أده لتسهيل وصولهم.

2. إن منتجو دعارة الأطفال وجدوا الانترنت كسوق واسع ومناسب لبيع منتجاتهم من المواد الخاصة بهذه الدعارة.

3. وجود مجرمين منجذبين نحو الأطفال والذين يسخّرون ضحاياهم بهدف الوصول إلى لقاءات حقيقية في الحياة ويستغلون الوسائل الالكترونية لتحقيق أهدافهم كالبريد الالكتروني أو غرف التخاطب أو من خلال المراسلة.[2]

كما أن هناك عوامل كثيرة تؤدي إلى حدوث الإستغلال الجنسي ومنها:[3]

1- عوامل اجتماعية:

هذه العوامل أكثر ما تكون ارتباطاً بعادات وتقاليد موروثة جعلت من الثقافة الجنسية عيباً لا يمكن الاقتراب منه مما حدى بالأطفال و صغار السن نحو شبكة الانترنت التي توفر لهم مساحة كبيرة من الحرية, حيث لا رقيب عليهم بالصورة المبتغاة لحمايتهم من الوقوع في مواقع إباحية فيتعلمون منها بطريقه التقليد دون إدراك لخطورة الأمر.

---

[1] الشوابكة . محمد أمين . مرجع سابق ص105

[2] هروال,نبيلة هبة(2006).**الجوانب الإجرائية لجرائم الإنترنت**.الاسكندرية:دار الفكر الجامعي. ص67

[3] الحمود,وضاح,والمجالي,نشأت ,مرجع سابق,ص63 وما بعدها

2- عوامل سياسية:

للسياسة نصيب في حدوث العنف ضد الأطفال وخاصة ما يحدث من استغلال جنسي بشع, إذ أن السياسة ولدت الحروب وفي الحروب تزداد الجريمة بصورة عامة , وهناك ما يسمى بالحروب الباردة التي يهدد فيها الأعداء ويتوعدون بشتى الطرق والوسائل وأهمها التي استخدمت بطريقه مباشرة لهدم الأخلاق العامة ومحاربة كل ديانه ملتزمة لتحطيم المجتمعات وخاصة الأطفال إذ أنهم هم المستقبل.

3- عوامل اقتصادية:

إن العوامل الاقتصادية تدفع الفقراء إلى بيع أجسادهم من اجل لقمة العيش, بل وتدفع تجار البغاء والجنس غير المشروع للتوجه إلى تلك المناطق من أجل اصطياد ضحاياهم وهم يستغلون شبكة الانترنت للإتصال مع وسطاء لهم, كما أن هؤلاء الوسطاء ليسوا غريبين بل هم في اغلبهم من داخل تلك البلدان الفقيرة المعدمة يتولون الوساطة وفتح المزادات على اغلي وأثمن جوهرة يمتلكها العالم وهي الطفل البريء.[1]

وقد جرمت معظم دول العالم الاستغلال الجنسي للأطفال في تشريعاتها ,ومنها قانون حماية الطفل المصري في المادة (116) والمادة 227 من قانون العقوبات الفرنسي، في بنودها (23 و24 و25 و26 و27-1 و27-3) بحيث أصبحت تعاقب مرتكبي جرائم الإباحية ودعارة

[1] الحمود,وضاح,والمجالي,نشأت ,مرجع سابق,ص63

الأطفال على الإنترنت مثل جرائم العمل على انحراف القاصر وانتاج وبث صور وكتابات ذات طابع عنيف أو اباحي وجرم تخبئة الصور الخلاعية التي تتناول الأطفال كحفظها على أقراص مدمجة أو غيرها من وسائل الحفظ والتسجيل)[1], وما أوردته الاتفاقية الدولية الخاصة بالإجرام المعلوماتي بما فوض في الفصل التاسع من الاتفاقية إلى الدول المتعاقدة اتخاذ النصوص الضرورية لتجريم إنتاج الصور الجنسية للأطفال لغاية بثها بواسطة الأنظمة المعلوماتية أو عرضها أو توزيعها أو نقلها أو التوّصل بها أو تخزينها, حيث اعتبرت الاتفاقية ان الطفل هو كل شخص لم يتجاوز الثامنة عشر من عمره[2]

المطلب الثاني

موقف المشرع الأردني من جرائم الاستغلال الجنسي للأطفال

شدد المشرع الأردني إجراءات حماية الأطفال والأحداث ومن لم يبلغوا الثامنة عشر من العمر من الاستغلال الجنسي عبر أنظمة المعلومات والانترنت فقد نصت المادة 8 من قانون جرائم أنظمة المعلومات المؤقت على انه:

(أ. كل من أرسل أو نشر عن طريق نظام معلومات أو الشبكة المعلوماتية قصدا كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالاً إباحية يشارك فيها أو تتعلق بالاستغلال الجنسي لمن لم يكمل الثامنة عشرة من العمر يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن (300) ثلاثمائة دينار ولا تزيد على (5000) خمسة الآف دينار.

---

[1] الشاعر,نضال,(2005) **حماية الأطفال من سوء استخدام الإنترنت وجرائم المعلوماتية**, متاح: www.atfalouna.gov.lb/Files/nt4.doc

[2] كحلون,علي(2005), **المسؤولية المعلوماتية**,مركزالنشرالجامعي, ص 171

ب. كل من قام قصدا باستخدام نظام معلومات أو الشبكة المعلوماتية في إعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية لغايات التأثير على من لم يكمل الثامنة عشرة من العمر أو من هو معوق نفسيا أو عقليا ، أو توجيهه أو تحريضه على ارتكاب جريمة ، يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة الآف دينار.

ج. كل من قام قصدا باستخدام نظام معلومات أو الشبكة المعلوماتية لغايات استغلال من لم يكمل الثامنة عشرة من العمر أو من هو معوق نفسيا أو عقليا ، في الدعارة أو الأعمال الإباحية يعاقب بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (5000) خمسة الآف دينار ولا تزيد على (15000) خمسة عشر ألف دينار).

حيث جرمت المادة (8) من هذا القانون عدة جوانب من الجرائم الموجهة ضد الأطفال ابتداء بعرض أي مواد إباحية وتوزيعها على من هو دون الثامنة عشر ولو كانت تلك المواد لا تخص أحداثا، كما تجرم كل تصرف يتعلق بمواد جنسية متعلقة بالأحداث أو توجه إليهم، إضافة إلى عرض تقديم مثل هذه المواد كما تشمل هذه المادة كل ما يخص أو يوجه إلى أو يمس الحدث بشكل عام كقيام شخص بالإعلان عن حيازته مثل هذه المواد عبر شبكة المعلومات أو طلب مثل هذه المواد أو قام بتصميم موقع لاستقبال مثل هذه المواد.

كما تحمي المادة (8) مصالح متعددة فهذه المادة هدفها حماية الحدث من التعرض للاعتداء وتحميه من التصرفات التي قد تسبب له الأذى النفسي كما تحميه من الأفعال التي تشجعه على الخروج عن قواعد الأخلاق أو تدفعه لارتكاب أفعال تخرج عن مفهوم الحياء أو تتعلق باعتداء جنسي عليه أو تدفعه لارتكاب جريمة.

ومن الواضح أن التجريم يشمل نشر أية مادة مكتوبة أو مقروئه أو صورة أو أكثر لحدث من خلال شبكة المعلومات أو نظام المعلومات أو الإشارة لمواقع تنشر مثل تلك المواد أو امتلاك نظام معلوماتي يحتوي تلك المواد, وبالإضافة لكون البند (ا) من المادة (8) من القانون يجرم إرسال أو نشر ما هو مخل بالحياء لحدث فإنها تجرم نشر أو إرسال ما يخص الحدث ويشمل الصور والتسجيلات الصوتية والفيديوية وغيرها والخاصة بالحدث دون اعتبار لوجود أو عدم وجود رابطة ما بين الفاعل والحدث ودون تمييز بين أن يكون الفعل موجها للجمهور أم لا , وقد ترك تعريف الحياء بشكل عام لسلطة قاضي الموضوع المستندة للمعايير المحلية والبيئة الأسرية داخل المملكة ومن المعروف ان ما يعتبر مناف للحياء لو عرض علي من تجاوز سن الثامنة عشر قد يعتبر مناف للحياء لما دون ذلك السن وذلك لما يحدثه من اثر نفسي وأخلاقي تجاهه .

والحقيقة انه يتصور وقوع أفعال حض الحدث على الانحراف الجنسي من خلال شبكة الانترنت والتي تعد بمثابة غاية للحدث محدود المعرفة والإدراك, ومن المواد غير المرغوب فيها الصور أو المشاهد الإباحية وكذلك الإعلانات التي تعدم القيم عند الطفل.

ويقصد بالصورة الواردة في نص المادة (8) الصورة الشخصية أو صورة شمسية والسينما وكذلك النحت وأي تماثيل أخر لحدث أو طفل ولو كان خياليا, ذلك لان التجريم هنا مناطه أو موضوعه الاعتداء على الحدث والذي لم يقع بعد, أنما التجريم ينصرف إلي سلوك الجاني الذي يركز في مشروعه الإجرامي علي الإساءة للطفولة واستغلالها عن طريق استعمال وترويج صور جنسية أو ذات طابع جنسي تخص الأطفال .

وقد تدخل المشرع الأردني لحماية الأطفال من الاستغلال الجنسي لهم في مواضع تجريمية تقليدية مختلفة حيث بين في الفصل الثاني من الباب السادس من قانون العقوبات الأردني رقم (16) لسنة 1960 الجرائم التي تمس الأسرة في المواد من (287 –291) من هذا القانون والمتعلقة بجرائم الأطفال و العجز.

ولم يقف المشرع عند هذا الحد لحماية الأطفال حيث أورد نصوصا مختلفة تجرم الاعتداء على الأطفال فيما يتعلق بالتعرض للآداب والأخلاق العامة بصورتها التقليدية من نفس القانون المشار إليه, حيث نصت المادة (306)على انه:

(من عرض على صبى دون الخامسة عشرة من عمره او على أنثى عملاً منافياً للحياء او وجه إليهما كلاماً منافياً للحياء ، عوقب بالحبس مدة لا تتجاوز ستة أشهر او بغرامة لا تزيد على خمسة وعشرين ديناراً).

كما نصت المادة 320 على ان :(كل من فعل فعلا منافيا للحياء أو أبدى إشارة منافية للحياء في مكان عام أو في مجتمع عام أو بصورة يمكن معها لمن كان في مكان عام ان يراه ، يعاقب بالحبس مدة لا تزيد على ستة أشهر أو بغرامة لا تزيد على خمسين دينارا).

كما نصت المادة (310) على انه (يعاقب بالحبس من ستة أشهر الى ثلاث سنوات وبغرامة من مائتي دينار الى خمسمائة دينار كل من قاد أو حاول قيادة :–

1– أنثى دون العشرين من العمر ليواقعها شخص مواقعة غير مشروعة في المملكة او في الخارج ، وكانت تلك الانثى ليست بغياً او معروفة بفساد الاخلاق ,او

2– أنثى لتصبح بغياً في المملكة او في الخارج ، او

3- أنثى لمغادرة المملكة بقصد ان تقيم في بيت بغاء او ان تتردد إليه ، او

4- أنثى لتغادر مكان إقامتها العادي في المملكة ولم يكن ذلك المكان بيت بغاء ، بقصد ان تقيم في بيت بغاء في المملكة او في الخارج او ان تتردد اليه لاجل مزاولة البغاء ، او

5- شخص لم يتم الثامنة عشرة من عمره لارتكاب فعل اللواط به).

كما نصت المادة (8) من قانون منع الاتجار بالبشر رقم (9)لسنة 2009 على انه: (يعاقب بالحبس مدة لا تقل عن ستة اشهر او بغرامة لا تقل عن الف دينار ولا تزيد على خمسة الاف دينار او بكلتا هاتين العقوبتين كل من ارتكب احدى جرائم الاتجار بالبشر المنصوص عليها في البند (1) من الفقرة (أ) من المادة (3) من هذا القانون) حيث تم ايضاح معنى الاستغلال في المادة (3/ب) من نفس القانون بقولها (تعني كلمة (الاستغلال) استغلال الاشخاص في العمل بالسخرة او العمل قسرا او الاسترقاق او الاستعباد او نزع الاعضاء او في الدعارة او اي شكل من اشكال الاستغلال الجنسي) 0

وباستقراء نص المادة (306) نجدها تجرم عرض أعمال منافية للحياة وكذلك توجيه الكلام المنافي للحياء إلى الأطفال وبالرجوع إلى نص المادة (8/أ) نجدها تجرم أيضاً كل ما هو مسموع أو مقروء أو مرئي يتضمن اعمالاً إباحية تتعلق باستغلال الأطفال بحيث يعتبر الكلام المنافي للحياء في المادة (306) من قبيل ما هو مسموع أو مقروء أو مرئي في المادة (8/أ) من قانون جرائم أنظمة المعلومات .

وباستقراء المادة (310) من قانون العقوبات, وإذا أردنا رؤية مدى انطباق هذا النص على جريمة الدعارة عبر الانترنت على افتراض أن شبكة الانترنت هي عالم افتراضي فقد يحدث

تعارف بين شخصين وعلى سبيل المثال في غرف المحادثة وبدون تهديد أو تخويف أو مخادعه يتم العرض من أحد الطرفين بالإيجاب والقبول على عرض القيام بالمواقعه الغير مشروعه وبعدها يتم الاتفاق على الكيفية والمكان في المملكة أو في الخارج, سواء أكانت الأنثى دون العشرين من العمر وليست بغيا أو معروفه بفساد الأخلاق أو لتصبح بغيا في المملكة أو في الخارج .

كذلك و باستقراء المادة (320) من قانون العقوبات و بالنظر إلى طبيعة أنظمة المعلومات نجدها تشكل مجتمعا عاماً افتراضيا يمكن من خلاله تبادل البيانات فإن أي فعل منافيا للحياء يرتكب من خلالها يشكل جريمة التعرض للأخلاق و الآداب العامة.

وباستقراء نص المادة (8) من قانون منع الاتجار بالبشر نجدها تعاقب على استغلال من هم دون الثامنة عشر في الدعاره كذلك جاءت المادة (3/ب) بعبارة فضفاضه وهي (أو اي شكل من اشكال الاستغلال الجنسي) بحيث يدخل ضمن طياتها الاستغلال الجنسي للأطفال باستخدام النظام المعلوماتي والشبكة المعلوماتية .

و يثور التساؤل هنا عن مدى انطباق هذه النصوص التقليدية عما يرتكب من جرائم تمس الأطفال باستخدام أنظمة المعلومات ؟

ومن تفحص النصوص السابقة نرى انه لا يمكن التوسع بها لمعالجة ما يقع من جرائم استغلال جنسي للأطفال عبر الانترنت, وذلك لأن العقوبة الواردة بالنص التقليدي متواضعة إلى حد كبير ولا تشمل أساسيات الردع العام والخاص المطلوبة, ولا تتناسب مع الخطورة الجرمية الظاهرة في نفس المجرم المعلوماتي الذي يقتحم أماكن تواجد الأطفال وأماكن ارتيادهم عبر الشبكة المعلوماتية للقيام بأفعال الإستغلال الجنسي لهم, كما أن هذه المواد

التقليدية لم تتطرق إلى تجريم استغلال من هو معوق نفسياً أو عقلياً في الدعارة أو الأعمال الإباحية كما جاءت به المادة (8/ج) من قانون جرائم أنظمة المعلومات, كذلك فإنه لا يمكن القياس في النصوص الجزائية ولا يمكن التوسع بها .

وعودة إلى إعمال الدعارة عن طريق شبكة المعلومات فالأمر لا يقتصر على حالات إنتاج صور إباحية فقط ونشرها أو بثها أو تداولها, حيث يمكن إفساد القاصر أو دفعه للإنحراف عن طريق اشتراكه في منتديات الحوار أو غرف الدردشة, وكذلك البريد الالكتروني وذلك من خلال المعلومات الجنسية المغلوطه التي يتلقاها دون رقيب أو بسوء نية ممن يتولى مخاطبته أو تزويده بهذه المعلومات.[1]

ولقيام هذه الجريمة لابد من توافر القصد الجرمي لدى الفاعل, ويقوم عنصر العلم على أن الفعل أو القول مضمون العرض على الصبي أو الكلام هو منافٍ للحياء والآداب العامة و أن تنصرف إرادته إلى إتيانه ,أما إذا وقع الفعل عرضا من غير قصد فينتفي عنصر إرادة الفعل.[2]

[1] حجازي,عبد الفتاح بيومي,مرجع سابق, ص 139

[2] الجبور,محمد عودة(2000).**الجرائم الواقعةعلى الأشخاص**,ط1.دن.ص340

المبحث الثاني

جريمة الترويج للدعارة عبر النظام المعلوماتي

الإنترنت إلى جانب صورته المشرقة والايجابية في حياة الأشخاص, إلا أن من آثاره السلبية على الأحداث والبالغين تتمثل بتزويدهم بمعلومات ضارة وغير نافعة تؤدي في النهاية إلى إفساد أخلاقهم أو دخولهم في علاقات غير مشروعة تنتهي إلى أن يكونوا مجرمين أو مجني عليهم في جرائم العرض وإفساد الأخلاق.[1]

[1] حجازي ,عبد الفتاح بيومي,مرجع سابق , ص124

فقد دفعت وسائل التكنولوجيا بعض الجناة إلى محاولة استغلال التقدم العلمي في نشر وترويج العديد من المواد الإباحية الفاضحة, وقيامهم بالأفعال الفاحشة و المخلة بالآداب والأخلاق العامة عبر الشبكة المعلوماتية, من أجل تحقيق أهداف شخصية أو تحقيق الربح المادي منها .

وللتعرف على هذه الجريمة ارتأيت إلى تقسيم هذا المبحث لمطلبين كالتالي:

المطلب الأول: ماهية جريمة الترويج للدعارة عبر النظام المعلوماتي.

المطلب الثاني: موقف المشرع الأردني من جريمة الترويج للدعارة عبر النظام المعلوماتي.

المطلب الأول

ماهية جريمة الترويج للدعارة عبر النظام المعلوماتي

يعني الترويج: نشر المعلومات وتوجيه مجموعة مركزة من الرسائل بهدف التأثير على آراء أو سلوك أكبر عدد من الأشخاص.[1]

وتتحقق تلك الجريمة من خلال العديد من الأفعال المادية التي تتجسد في عرض أو نشر أو توزيع أية صور أو أقوال أو أفعال جنسية فاحشة وفاضحة مخلة بالآداب العامة على الشبكة

[1] ويكيبيديا,2012, دعاوة,متاح: http://ar.wikipedia.org/wiki/%D8%AF%D8%B9%D8%A7%D9%88%D8%A9

المعلوماتية, وتتحقق تلك الجريمة أيضاً من خلال إنشاء المواقع الجنسية على شبكة الانترنت وإضافة المواد الفاضحة فيها كالصور الجنسية أو الفيديو أو حتى تأليف القصص ذات الأهداف الجنسية وعرضها على الأشخاص والترويج لها واستقطاب الزائرين إليها, وتتحقق أيضاً باستخدام البريد الإلكتروني كوسيلة لتبادل الرسائل التي تحتوي على العديد من الصور أو الإشارات أو الأقوال الفاضحة, كما و يمكن إستغلال البريد الإلكتروني للأشخاص من قبل المواقع الإباحية بحيث تتم عملية إرسال رسائل إباحية تحتوي على مواد فاحشة تكون مرفقه مع هذه الرسالة وغالباً ما تكون مجهولة المصدر.[1]

ويندرج تحت بند المواقع والقوائم البريدية الإباحية جرائم ارتياد المواقع الإباحية سواء أكان بهدف تصفحها أو الإشتراك فيها أو الشراء منها أو إنشائها[2].

وتختلف المواقع الإباحية عن القوائم البريدية التي تخصص لتبادل المواد الفاحشة من الصور والأفلام الجنسية في أن المواقع الإباحية غالباً ما يكون الهدف من إنشائها هو الربح المادي حيث تستوجب دفع اشتراك شهري أو سنوي أو دفع مبلغ معين مقطوع مقابل مشاهدة فيلم أو التصفح لوقت محدد, وتقوم هذه المواقع بالترويج عن موادها الإباحية عن طريق استدراج مرتديها بتقديم خدمة إرسال الصور الجنسية المجانية يومياً على بريدهم الإلكتروني[3].

أما القوائم البريدية فهي مجانية في الغالب وأسهل إنشاءاً ويقوم أعضائها من المشتركين بتبادل الصور والأفلام على عناوينهم البريدية, بحيث تكون هذه العناوين أبعد عن إمكانية المتابعة الأمنية لهم ويكون من الصعوبة منعها أو اكتشافها.[4]

[1] سلامه,محمد عبدالله,مرجع سابق,ص199
[2] الحسيناوي,علي جبار,مرجع سابق,ص95
[3] الحسيناوي,علي جبار,مرجع سابق,ص96
[4] الحسيناوي,علي جبار,مرجع سابق,ص96

كما أن مروجو الدعارة على شبكة الانترنت يستغلون كل تقنية متوفرة وكل وسيلة ممكنه لارتكاب جرائمهم, كما يستعملون أساليب الخداع والإغواء على شبكة الانترنت ومنها:

أولاً. مواقع المحادثة:[1]

وهي من أخطر الأماكن الموجودة على شبكة الانترنت حيث توفر بعض المواقع خدمة المحادثة ضمن مجموعات متنوعة, وقد تطورت هذه المحادثة من الكتابية إلى الصوتية ثم المرئية, فقد قام تجار الجنس باستغلال هذه الغرف والدخول إليها بأسماء وأعمار ومعلومات وهمية وذلك لاستدراج ضحاياهم, فتبدأ هذه المحادثة من مرحلة التعارف البسيط ثم يبدأ مجرمي الجنس غير المشروع سلسلة من الإغواءات والإغراءات المادية والنفسية والجنسية وغيرها من العروض إلى أن تقع الضحية في الفخ الذي اعد لها.

ثانياً. تزوير المواقع:

حيث يقوم تجار الجنس باستغلال أسماء المواقع التي يزورها أكبر عدد من الأطفال والمراهقين وحتى البالغين ايضاً, حيث يتم استخدام عنوان الموقع ولكن بعد تغيير حرف مكان حرف أو تبديلها بأحرف جديدة أو زيادة حرف أو رقم على اسم الموقع الأصلي, حتى يقع الضحية في خطأ طباعي ويدخل إلى هذا الموقع الجنسي.[2]

ثالثاً. الدعاية والإعلان:

---

[1] الحمود,وضاح,والمجالي,نشأت ,مرجع سابق,ص106

[2] الحمود,وضاح,والمجالي,نشأت ,مرجع سابق,ص107

حيث يتم استغلال التواجد الهائل من متصفحي الانترنت وذلك بعرض إعلانات على اختلاف أشكالها وبتقنية عالية تحفز الكثيرين على النقر على هذا الإعلان, وبمجرد حصول ذلك تبدأ سلسلة من الخداع إلى أن يتم الوقوع في شبكة الجنس غير المشروع.

رابعاً. المجموعات الإخبارية:

هي عبارة عن ساحات تخّول الجمهور صلاحية التحدث حول مواضيع مختلفة والمناقشة فيها مع إمكانية تبادل المعلومات كالصور والكتابة والأفلام, فهذه المجموعات هي ايضاً تقع ضمن اهتمامات تجار الجنس فيدخلون إليها ويشاركون ثم يختارون ضحاياهم واحداً تلو الآخر.[1]

خامساً. مواقع جنسية مباشرة:

وهذه المواقع موجودة بكثره على شبكة الانترنت ومنها ما هو مجاني وهي مثيرة للغريزة والشهوة الجنسية وهي بازدياد رغم مكافحتها, وتستعمل للترويج للدعارة وإفساد الأخلاق عن طريق بث الأفلام والصور الإباحية من خلالها.[2]

ومن الوسائل الأخرى التي يستخدمها مروجو الدعارة هي مواقع الكازينو والقمار ومواقع البحث عن شريك الحياة ومواقع فرص العمل ومواقع الألعاب للأطفال, كذلك فإن الأساليب عبر الانترنت كثيرة ومتنوعة ولم يترك تجار الرذيلة أي وسيلة أو طريقة أو منفذ إلا وقاموا باختراقه مما أساء إلى شبكة الانترنت.

وقد يتعدى الهدف من تلك الجرائم مجرد الترويج للدعارة فهناك من يستغل ذلك لعمليات الإحتيال المعلوماتي عن طريق إنشاء مواقع جنسية وهمية تهدف إلى الحصول على أموال

---

[1] الشوابكه,محمد امين,مرجع سابق,ص 31

[2] الحمود,وضاح,والمجالي,نشأت ,مرجع سابق,ص112

غير مشروعه عن طريق إيهام المستخدمين بوجود مواد إباحية قابلة للبيع وتجميع الأموال المتحصلة عن طريق الإشتراكات التي يدفعا المستخدمون, ويكون الهدف منها أحياناً إلحاق الضرر بمستخدمي الشبكة المعلوماتية عن طريق إتلاف المكونات المنطقية للحاسب الآلي باستخدام الفيروسات التي تكون مرفقة مع الملفات الجنسية عند تحميلها على جهاز الضحية والتي تؤدي في النهاية إلى اختراق ذلك الجهاز أو تدمير مكوناته.[1]

المطلب الثاني

موقف المشرع الأردني من جريمة الترويج للدعارة عبر النظام المعلوماتي

عالجت المادة (9) من قانون جرائم أنظمة المعلومات جريمة الترويج للدعارة باستخدام النظام المعلوماتي, حيث نصت على :

[1] سلامة'محمد عبدالله ,مرجع سابق,ص199

(كل من قام قصدا باستخدام نظام معلومات أو الشبكة المعلوماتية أو أي نظام للترويج للدعارة يعاقب بالحبس مدة لأتقل عن ستة أشهر وبغرامة لا تقل عن (300) ثلاثمائة دينار ولا تزيد على (5000) خمسة الإلف دينار).

وتهدف المادة (9) إلى منع استغلال التطور الهائل في تقنية المعلومات وشبكات المعلومات لارتكاب أو الترويج لجرائم الدعارة والفجور, فالترويج للدعارة والفجور (والتي يعالجها قانون العقوبات في الفصل الثاني – الحض على الفجور) يسهل ارتكابه من خلال الشبكة المعلوماتية التي يسهل الوصول للجمهور من خلالها، مما يحتم تشديد تجريم استخدام أنظمة المعلومات والشبكة المعلوماتية لهذه الغاية صراحة.

ويجدر بالذكر أن مجرد إرسال الصور المخلة بالحياء بين من تتجاوز أعمارهم ثمانية عشر عاما لا يقع تحت مفهوم هذه المادة ولم يتم تجريمه بهذا القانون منعا لاستغلاله في تقديم شكاوى وادعاءات كيدية، إضافة إلى كفاية النصوص الحالية بالنسبة لتجريم الأفعال التي تقع ضد من تتجاوز أعمارهم الثمانية عشر عاما، وعدم وجود حاجة لتشديدها إن ارتكبت بوسائل الكترونية.[1]

كذلك فإن أعمال الترويج للدعارة قد تم تجريمها في قانون العقوبات الأردني حيث نصت ألماده 319 على انه:

(يعاقب بالحبس مدة لا تزيد على ثلاثة أشهر أو بغرامة لا تزيد على خمسين دينارا كل من:1- باع أو أحرز بقصد البيع أو التوزيع أية مادة بذيئة مطبوعة أو مخطوطة أو أية

[1] المذكرة الايضاحية لقانون جرائم أنظمة المعلومات رقم (30) لسنة (2010) , ص7

صورة شمسية أو رسم أو نموذج أو أي شي آخر يؤدي إلى إفساد الأخلاق ، أو طبع أو أعاد طبع مثل هذه الأِشياء والمواد بقصد بيعها أو توزيعها.

2- عرض في محل عام أي تصوير أو صورة شمسية أو رسم أو نموذج بذيء أو أي شيء آخر قد يؤدي إلى إفساد الأخلاق ، أو وزع مثل هذه الأِشياء لعرضها في محل عام ، أو

3- أدار أو اشترك في إدارة محل يتعاطى بيع أو نشر أو عرض أشياء بذيئة مطبوعة كانت أو مخطوطة أو صورة شمسية أو رسوم أو نماذج أو أية أشياء أخرى قد تؤدي إلى إفساد الأخلاق.

4- أعلن أو أذاع بأية وسيلة من الوسائل ان شخصا يتعاطى بيع هذه المواد والأشياء البذيئة أو طبعها أو إعادة طبعها أو عرضها أو توزيعها).

باستقراء المادة 319 من قانون العقوبات الأردني نجد أن المشرع لا يعاقب على أحرز مواد بذيئة إلى إذا اتجهت النية لبيعها, سواء أكانت تلك المواد مخطوطه أو مطبوعة أو نموذجا أو صورا شمسية أو أي شيء آخر, فمثلا من حاز مواد إباحية في بريده الالكتروني الخاص دون أن تتجه نيته إلى بيعها فلا يعتبر مرتكبا لجريمة الإخلال بالآداب والأخلاق العامة, كذلك ويشمل التجريم كل من أعلن أو ذاع بأي وسيلة من الوسائل لبيع هذه المواد أو طبعها أو عرضها أو توزيعها أو إدارة محل يتعاطى بيع أو نشر أو عرض أشياء بذيئة, وحيث أن المشرع استخدم ألفاظ موسعة وذلك بقوله (بأي وسيلة من الوسائل) بحيث يشمل هنا أي وسيلة حديثة ومنها شبكة الانترنت فهي من الوسائل الحديثه التي يتم استخدامها للإعلان والإذاعه بصورة عالية الجودة تجلب اعداداً كبيرة من الزبائن.

كما أن الحاسب الآلي يمكن استخدامه لتخزين العديد من المواد البذيئة والمطبوعه أو المخطوطة أو الرسوم, وكذلك من خلال شبكة الانترنت فإن إمكانية التوزيع لا تتطلب الجهد الكبير, حيث أن التوزيع فيها يتعدى الحدود الجغرافية لأي دوله بسهولة , كما أن المشرع قد جرم ايضاً عرض المواد البذيئة في محل عام وتمكين آخرين من مشاهدتها, وفي وقتنا الحالي فلا يكاد يخلو شارع من مقاهي الانترنت ويقوم بعض أصحاب هذه المقاهي بالسماح بالدخول على مواقع جنسية غير مشروعة.

و يثور التساؤل هنا عن مدى انطباق النص التقليدي عما يرتكب من جرائم باستخدام أنظمة المعلومات؟

باستقراء نصوص المواد السابقة نجد أن المادة (319) من قانون العقوبات لم تعالج صراحة جريمة الترويج للدعارة باستخدام النظام المعلوماتي بل أنها عالجت ما يقع من جرائم ترويج للدعارة بشكل تقليدي دون التطرق للنظام المعلوماتي, وبما أن المادة (9) من قانون جرائم أنظمة المعلومات قد جاءت بنص خاص يعالج جريمة الترويج للدعارة في حال ارتكبت بواسطة الشبكة المعلوماتية أو النظام المعلوماتي فإن نص المادة (9) هو الواجب التطبيق في هذه الحالة, وذلك لأن النص الخاص يقيد النص العام, كما أن العقوبة في المادة (319) هي الحبس مدة لا تزيد عن ثلاثة أشهر أو الغرامة التي لا تزيد عن خمسين دينار وهي عقوبة متواضعة بالنسبة إلى حجم الجريمة ولا تشكل أساس الردع العام, أما المادة (9) فإن العقوبة فيها الحبس مدة لا تقل عن ستة أشهر و غرامة من(300 إلى 5000) دينار.

والحقيقة أن نص المادة (9) يثير كذلك عدة تساؤلات حول مسؤولية كل من مزودي خدمة الانترنت ومسؤولية مقدمي الخدمة عن ما يتم تداوله من مواد بذيئة تؤدي إلي فساد أخلاقي

خاصا أن مزودي خدمة الانترنت ومقدمي تلك الخدمة يديرون ويشتركون في أدارة مقاهي الانترنت التي يمكن من خلالها أن يقوم مستخدمي الشبكة بإجراء عمليات المبادلات الالكترونية من بيع أو شراء مواد بذيئة ونشرها أو عرضها سواء أكانت مطبوعة أو محفوظة (القرص المدمج)[1].

إن المشرع الأردني قد نص في المادة (75) من قانون الاتصالات بند (ب) رقم (13) لسنة 1995 على أن (كل من قام أو ساهم بتقديم خدمات اتصالات مخالفة للنظام العام أو الآداب العامة يعاقب بالعقوبات المنصوص عليها في الفقرة (ا) من هذه المادة بالإضافة إلي تطبيق الإحكام المنصوص عليها في المادة (40) من هذا القانون).

ويتبين من نص المادة (75) أن المشرع الأردني يقيم المسؤولية الجنائية لمزودي ومقدمي الانترنت باعتبارها من خدمات الاتصالات أذا قاموا أو ساهموا بتقديم خدمات اتصال مخالفة للنظام العام أو الآداب العامة, وقد فرض المشرع العقوبات المنصوص عليها في ذات المادة 75 فقرة (ا) والمتمثلة في الحبس مدة لا تقل عن شهر ولا تزيد علي سنه أو بغرامة لا تزيد علي (200) دينار أو بكلتا العقوبتين .

وإذا كانت المادة (75) من قانون الاتصالات تقيم المسؤولية على من يقدم أو يساهم في تقديم خدمة اتصالات تخل بالنظام العام والآداب العامة فهنا تصبح الشركات المزودة لخدمة الانترنت لا تقع عليها مسؤولية مراقبة الشبكة بالكامل فلابد أن يضع المشرع ضوابط محددة ومنظمة لتلك الشركات تلزمهم بفحص محتوي خدماتهم .

---

[1] الشوابكة .محمد . أمين . مرجع سابق .ص 110

ويمكن أقامة الدليل علي المواقع المصدرة للمواد الإباحية من خلال برمجة الأنظمة المزودة في الشركات مزودة الخدمة لتستنسخ الملفات المحتوية علي المواد الإباحية واستخدامها عند أقامة الدليل.

ومن الأمثلة الواقعية ما وجهه مدعي عام عمان من تهمة " ممارسة أعمال الدعارة الإلكترونية والترويج لها ونشر صور فاضحة بقصد ممارسة أعمال الدعارة، ومخالفة قانون المعاملات الإلكترونية" من خلال موقع الكتروني لثلاثة أشقاء أحدهم فار من وجه السلطات, حيث تلقت مديرية الأمن العام عبر بريدها الإلكتروني رسالة من أحد المواطنين يؤكد فيها "وجود موقع إلكتروني إباحي" وبعد متابعة الشكوى بشكل علمي وفني دقيق تم التوصل إلى المشتبه بهم الذين كانوا يديرون الموقع من منزلهم وكانوا يعرضون عليه صورا إباحية لفتيات وأرقام هواتف خلوية كما أنهم كانوا يتقاضون أموالاً لقاء هذه الأفعال بالتنسيق مع بائعات هوى إلى أن وقع أحدهم في كمين محكم نصبته له الأجهزة الأمنية, حيث ذكرت المصادر أن هذه هي أول قضية دعارة الكترونية تسجل في المملكة.[1]

الفصل الرابع

جرائم الإرهاب والإطلاع على أسرار الدولة

بات الأمر يسيراً على الإرهابيين في استخدام الشبكه المعلوماتية في تنفيذ أي عمل داخل أو خارج الإقليم من خلال الإعلان عن ذلك عبر شبكة الانترنت والاتصال ببعض المنظمات

[1] عين نيوز,2011, أول قضية دعارة الكترونية في الأردن,عين نيوز,متاح: http://ainnews.net/?p=60386.

الدولية لاستعراض خطط تنفيذ العمل الإجرامي والاتفاق على مكانه وزمانه, مع العلم بأن هناك العديد من المواقع الإجرامية المعلنة عبر شبكة الانترنت مخصصه لمنظمات إجرامية محترفة في جميع أعمال العنف والإرهاب[1], ويستخدم الجناة شبكة الانترنت أيضاً من أجل الحصول على معلومات تتعلق بأمن وسلامة الدولة بهدف الإضرار بمصالح تلك الدولة.

تقسيم:

سنعمل على تقسيم هذا الفصل إلى مبحثين؛ نعرض في المبحث الأول جرائم الإرهاب الإلكتروني التي تقع باستخدام أنظمة المعلومات والمنصوص عليها في المادة (10) من قانون جرائم أنظمة المعلومات رقم (30) لسنة 2010 ؛ ثم نتناول بعد ذلك في مبحث ثاني جرائم الإطلاع والعبث بالبيانات والمعلومات المتعلقة بأسرار الدولة والمنصوص عليها في المادة (11) من نفس القانون , وعلى ذلك فقد ارتأيت إلى تقسيم الفصل الرابع من الدراسة كالتالي:

المبحث الأول: الإرهاب الالكتروني.

المبحث الثاني: حماية أسرار الدولة.

المبحث الأول

الإرهاب الالكتروني

يعد التشريع أمراً مهماً وجوهرياً في مكافحة الجريمة الإرهابية, حيث وسع المشرع من نطاق التجريم ليمتد ويطال المنابع والوسائل التي من الممكن أن تؤدي إلى تسهيل ارتكاب الجريمة

[1] عياد, سامي حامد(2008),**استخدام تكنولوجيا المعلومات في مكافحة الإرهاب**.ط1.الاسكندرية:دار الفكر الجامعي.ص58

الإرهابية,[1] فقد تم تجريم استخدام أنظمة المعلومات بهدف تسهيل القيام بأعمال إرهابية أو تقديم الدعم للمنظمات أو الجماعات الإرهابية أو الترويج لإتباع أفكارهم باستخدام الشبكة المعلوماتية أو البريد الإلكتروني, وهذا ما نصت عليه المادة العاشرة من قانون جرائم أنظمة المعلومات. فقد استخُدم الإرهاب كنظام قائم على الرعب ضمن الشبكة المعلوماتية في تنفيذ العديد من الأعمال الإرهابية التي روعت أمن المواطن وأمن الدولة, واستعار الإرهابيون بهذه الوسيلة الآمنة في نشر ما يعرف بالرعب الالكتروني باعتباره احد الأبعاد الجديدة للإرهاب التقليدي.[2]

ومن الممكن عرض النظام القانوني للمواجهة التشريعية لجريمة الإرهاب من خلال التعريف بهذه الجريمة وذكر أركانها وخصائصها ومن ثم البحث في موقف المشرع الأردني من جريمة الإرهاب الإلكتروني.

وعليه سوف نقسم هذا المبحث إلى مطلبين كالتالي:

المطلب الأول: ماهية جريمة الإرهاب.

المطلب الثاني:موقف المشرع الأردني من جريمة الإرهاب الإلكتروني.

المطلب الأول

ماهية جريمة الإرهاب

[1] الهويدي,عمر سعد,مكافحة جرائم الإرهاب,دار وائل للنشر,عمان,2011,ط1, ص12
[2] عياد.سامي حامد,مرجع سابق,ص64

إذا كان التقاء الإرهابيين والمجرمين في مكان معين لتعلم طرق الإرهاب و الإجرام و تبادل الآراء والأفكار والمعلومات صعبا في الواقع فإن الانترنت قد سهل هذه العملية كثيراً, إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة في وقت واحد ويتبادلون الحديث والاستماع لبعضهم عبر الانترنت, بل يمكن أن يجمعوا لهم أتباعاً وأنصاراً عبر إشاعة أفكارهم ومبادئهم من خلال مواقع الانترنت ومنتديات الحوار وغرف الدردشة, فإذا كان الحصول على وسائل إعلامية كالقنوات الفضائية والإذاعية أمراً صعباً, فإن إنشاء مواقع على الانترنت واستغلال منتديات الحوار وغيرها لخدمة أهداف الإرهابيين أصبح سهلاً وممكناً,[1] بل تجد لبعض المنظمات الإرهابية آلاف المواقع حتى يضمنوا انتشاراً أوسع وحتى لو تم منع الدخول على بعض هذه المواقع أو تعرضت للتدمير تبقى المواقع الأخرى يمكن الوصول إليها , فقد وجد الإرهابيون بغيتهم في تلك الوسائل الرقمية في ثورة المعلومات فأصبح للمنظمات الإرهابية العديد من المواقع على شبكة الانترنت حيث أصبحت من أبرز الوسائل المستخدمة في الإرهاب الالكتروني.

وسنعمل على تقسيم هذا المطلب إلى الفروع الآتية:

الفرع الأول: تعريف الإرهاب

الفرع الثاني: خصائص الجريمة الإرهابية

الفرع الثالث: الركن المادي و الركن المعنوي في جريمة الإرهاب الإلكتروني

الفرع الأول

---

[1] عياد.سامي حامد,مرجع سابق,ص58

تعريف الإرهاب

إن التعريف التقليدي للجريمة الإرهابية يذهب إلى القول بأنها: كل عمل يرتكب بوسيلة فتاكة يبعث الذعر ويشكل خطراً عاماً يهدد أكثر من شخص.[1]

أما الإرهاب الإلكتروني فيمكن تعريفه بأنه: استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين, أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية واقتصادية وأمنية أو عرقية أو دينية.[2]

وقد عرفت المادة (1/147) من قانون العقوبات الأردني الإرهاب بقولها: (يقصد بالإرهاب : استخدام العنف بأي وسيلة كانت أو التهديد باستخدامه ، أياً كانت بواعثه وأغراضه ، يقع تنفيذاً لمشروع اجرامي فردي أو جماعي يهدف الى تعريض سلامة المجتمع وأمنه للخطر إذا كان من شأن ذلك إلقاء الرعب بين الناس وترويعهم أو تعريض حياتهم للخطر أو الحاق الضرر بالبيئة أو المرافق والأملاك العامة أو الأملاك الخاصة أو المرافق الدولية او البعثات الدبلوماسية أو باحتلال أي منها أو الاستيلاء عليها أو تعريض الموارد الوطنية للخطر او ارغام أي حكومة او أي منظمة دولية او اقليمية على القيام بأي عمل او الامتناع عنه).

كما عرف قانون منع الإرهاب رقم (55) لسنة 2006 العمل الإرهابي بأنه : (كل عمل مقصود يرتكب بأي وسيلة كانت يؤدي إلي قتل إي شخص أو التسبب بإيذائه جسديا أو إيقاع إضرارا في الممتلكات العامة أو الخاصة أو في وسائط النقل أو البنية التحتية أو في مرافق

---

[1] الجبور,محمد عودة(2010).**الجرائم الواقعة على أمن الدولة وجرائم الإرهاب**,ط2.عمان:دار الثقافة.ص336

[2] الزنط.سعد عطوة(2010). (الارهاب الالكتروني واعادة صياغة استراتيجيات الامن القومي).مؤتمر الجرائم المستحدثه.للفترة من 15-16 ديسمبر . المركز القومي للبحوث الاجتماعية والجنائية .القاهرة.مصر.

الهيئات الدولية أو البعثات الدبلوماسية أذا كانت الغاية منه الإخلال بالنظام العام وتعريض سلامة المجتمع وأمنه للخطر أو تعطيل أحكام الدستور أو القوانين أو التأثير علي سياسة الدولة أو الحكومة أو إجبارها علي عمل ما أو الامتناع عنه أو الإخلال بالأمن الوطني بواسطة التخويف أو الترهيب أو العنف) .

الفرع الثاني

خصائص الجريمة الإرهابية

يمكن لنا من تعريف الإرهاب واستخلاص العناصر الجوهرية التي يقوم عليها وهي:

1. استخدام العنف أو التهديد باستخدامه , فالعنف في الجريمة الإرهابية يشمل أعمال الإيذاء النفسي والبدني ويتحقق الأذى البدني حين يكون هناك مساس خطير بحياة الإنسان أو سلامة بدنه, أما العنف النفسي فيكمن في إلحاق الآماً واضطرابات نفسية من خلال الإشاعات التي تسبب القلق و الرعب بين الأفراد [1].

أما في حالة ارتكاب جريمة إرهابيه بواسطة أنظمة المعلومات فإنه لا يتصور وقوع أعمال عنف مادي, لأنه من خصائص هذه الجريمة أنها لا تحتاج للعنف للقيام بها , لكن يمكن تحقيق العنف الالكتروني باستخدام أسلوب الهجوم على شبكات المعلومات عن طريق توجيه مئات الآلاف من الرسائل الإلكترونية إلى مواقع هذه الشبكات مما يزيد الضغط على قدرتها على استقبال الرسائل من المتعاملين معها مما يؤدي إلى توقيف عمل الشبكة, وهذا يوحي

---

[1] الجبور . محمد عودة , مرجع سابق, ص337

بإمكانية استخدام القوة والعنف من خلال استخدام الانترنت في شن هجمات إرهابية لتدمير وإتلاف أنظمة المعلومات التي تعتمد عليها الدول المتقدمة في إدارة شؤونها السياسية والاقتصادية والاجتماعية.[1]

2. جريمة الإرهاب لا ترتكب إلى بعد تخطيط وتدبير مسبقين, ولا تأتي بشكل عفوي أو عن طريق الصدفة, حيث تتصف الجريمة الإرهابية بالتنظيم وبعدها عن العشوائية.

وفي مجال المعلوماتية يتصور التدبير والتخطيط في إنشاء مواقع الكترونية من قبل إحدى المنظمات الإرهابية وإضافة محتويات في هذا الموقع من أجل الترويج لاتباع أفكارها, كما يتصور في حالة التحويل الإلكتروني للأموال عبر البنوك الإلكترونية من دولة إلى أخرى وتستخدم هذه الطريقه –التحويل الالكتروني– لاتصافها بالسرعة والسرية بحيث يصعب اكتشافها [2].

3. من سمات الإرهاب بأنه عمل يقوم أساس مذاهب دينية وطائفية وفكرية متطرفة فهو عمل من أعمال العنف أو إجراء يتخذ من أجل التهديد به.

[1] عياد.سامي حامد,مرجع سابق,ص71
[2] الهويدي,عمر سعد,مرجع سابق, ص37

الفرع الثالث

الركن المادي و الركن المعنوي في جريمة الإرهاب الإلكتروني

اولاً: الركن المادي.

تتعدد صور وأنماط الركن المادي في جرائم الإرهاب الالكتروني وهي تتحقق بتوافر إمكانية إيقاع الفعل باستخدام تقنية أنظمة المعلومات, وأن يرتبط النشاط موضوع الفعل بنطاق الكتروني لتحقيق التجسيد المادي للفكر الإجرامي الباطني.

ويتكون الركن المادي لأية جريمة من عناصر ثلاثة وهي:

1. الفعل الإجرامي : ومن الممكن شرح الفعل الإجرامي بناءً على نص المادة العاشرة من قانون جرائم أنظمة المعلومات وذلك عند استخدام الجاني لأنظمة المعلومات, بحيث تكون هي الأداة أو الوسيلة التي تستخدم في ارتكاب الأفعال الإرهابية, فيقوم الجاني بإنشاء موقع الكتروني على شبكة الانترنت بهدف تمهيد الطريق للقيام بأعمال إرهابية كالترويج لاتباع أفكار إرهابية تحت مسميات دينية أو فكرية متطرفة أو التطرف والعنصرية أو التحريض عليها أو وضع المؤامرات التي تثير الفتنه في المجتمع و تنال من مكانة الدولة, حيث يمكن من خلال الانترنت بث الأفكار المتطرفة سواء كانت سياسية أو دينية والتي من شأنها أن تسيطر على وجدان الأفراد وإفساد عقائدهم , فهذه الأعمال و غيرها يستطيع الجاني تدوينها في موقعه الالكتروني لتسهيل القيام بالأعمال الإرهابية[1].

---

[1] عياد.سامي حامد,مرجع سابق,ص79

ويتحقق الفعل الإجرامي أيضاً في حال قيام الجاني بتقديم الدعم لجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية وتمويلها باستخدام الشبكة المعلوماتية, حين يقوم بتحويل الأموال الإلكترونية الموجودة في رصيده إلى رصيد إحدى الجماعات الإرهابية عن طريق البنوك الإلكترونية ومن أمثلتها البنك الشهير المسمى (PayPal).

2. النتيجة الجرميه:

تتمثل النتيجة الجرميه في التغيير الذي يطرأ على العالم الخارجي جراء احد الأفعال الإرهابية المتعلقة بالاعتداء على مصلحة محمية بموجب القانون, وهي تتحقق في حالتين وهما :

حالة الإضرار الفعلي للمصلحة المحمية من خلال تعطيلها كلياً أو إنقاصها وفي حالة تعريض تلك المصالح للخطر, وقد ذهب جانب من الفقه للتوسع في مفهوم النتيجة الإجرامية وذلك أنه لابد من أن يؤدي استخدام العنف أو التهديد (السلوك) إلى إحدى تلك النتائج وهي إلقاء الرعب بين الناس أو تعريض أمنهم للخطر أو إلحاق الضرر بالبيئة أو تعريض الموارد الوطنية للخطر أو أن يؤدي إلى تعطيل تطبيق أحكام الدستور والقوانين.

كما وتشغل النتيجة حيزاً مهما في الجريمة الإرهابية وذلك فيما يحدثه هذا السلوك من أثر في المجتمع و ركائز الدولة ودون وضع اعتبار للقوة المستخدمة ذاتها في تحقيق ذلك السلوك.[1]

3.العلاقة السببية:

يجب أن تكون هنالك رابطة ما بين السلوك الإجرامي و النتيجة الجريمة أي أن يكون الضرر الناشئ عن الجريمة ناتجاً عن سلوك الفاعل, فإذا قام احد الأشخاص بتأسيس موقع الكتروني للقيام بأعمال إرهابية ولم يضف في محتواه أي مواد لتسهيل القيام بالجريمة وحدث وان وقعت

[1] الهويدي,عمر سعد,مرجع سابق ص79

إحدى الجرائم الإرهابية في تلك الفترة فلا يمكن إسناد الجرم إليه بناءً على ذلك لأنه لا يوجد علاقة سببيه بين ما قام به وبين الجريمة الواقعة.

ثانياً : الركن المعنوي.

الجريمة الإرهابية هي جريمة مقصودة فلا يمكن أن تقع عن طريق الخطأ, كذلك يشترط لقيامها توافر عنصرين وهما العلم والإرادة ويكون العلم بعلم الجاني بعناصر جريمته أي العلم بماهية فعله والوسائل المستخدمة في ذلك فيجب توافر العلم حين دخول الجاني إلى الشبكة المعلوماتية وإنشاء موقع يسهل القيام بالأعمال الإرهابية, وكذلك يجب أن تتوجيه إرادته إلى ارتكاب هذا الفعل الإرهابي دون إكراه, حيث لا يكفي القصد العام لقيام الركن المعنوي في جرائم الإرهاب الالكتروني وإنما يلزم لقيامه قصدا خاص وهو إرادة ارتكاب السلوك المجرم بقصد تحقيق أحد الأغراض الجرمية الإرهابية. [1]

فلابد أن يتوافر في نية الفاعل وهو يقدم علي استخدام تقنية نظم المعلومات أن يوقع أو يهدد بإيقاع أحد الإغراض المعلنة في نص التجريم لما سيقدم عليه من فعل الكتروني, فان لم يتوافر ذلك لم تقم الجريمة. [2]

وأوضحت المذكرة التفسيرية لقانون جرائم أنظمة المعلومات مدلول عناصر القصد في جريمة أنظمة المعلومات وبينت أنها تنصب على (العلم بأن الفعل سوف يؤدي إلى أحد الأفعال المجرمة بموجب هذا القانون وإن العمد فيها ينطوي على خطورة جرميه أكبر من حيث التحضير والتخطيط والتنفيذ).

---

[1] الهويدي,عمر سعد,مرجع سابق ص87
[2] الزعبي,جلال,والمناعسه, محمد. مرجع سابق .ص28

المطلب الثاني

موقف المشرع الأردني من جريمة الإرهاب الإلكتروني

جاءت المادة (10) من قانون جرائم أنظمة المعلومات رقم (30) لسنة 2010 لتعالج بشكل خاص الجرائم الإرهابية الواقعة باستخدام أنظمة المعلومات حيث نصت على أنه :

(كل من استخدم نظام المعلومات أو الشبكة المعلوماتية أو انشأ موقعا الكترونيا لتسهيل القيام بأعمال إرهابية أو دعم لجماعة وتنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لاتباع أفكارها أو تمويلها يعاقب بالأشغال الشاقة المؤقتة).

ومن صياغة النص نجد أن المادة المذكورة تهدف إلي استمرار الجهود لمحاربة الإرهاب بكافة أشكاله وصوره بما في ذلك الترويج ونشر أفكاره والدعاية له بكافة السبل والوسائل بما في ذلك استخدام الوسائل الالكترونية .

كما أوضحت المادة (148) من قانون العقوبات, العقوبات المقررة لمرتكبي الجرائم الإرهابية وأوضحت نطاق التجريم والعقاب والظروف المشددة للعقوبة علي النحو الأتي:

فقد نصت المادة (1/148)من قانون العقوبات على انه (المؤامرة التي يقصد منها ارتكاب عمل أو أعمال إرهابية يعاقب عليها بالأشغال الشاقة المؤقتة) ونصت ذات المادة في الفقرة الثانية على (كل عمل إرهابي يستوجب الإشغال الشاقة خمس سنوات).

وجاءت الفقرة الثالثة والرابعة من المادة (148) لتشديد العقوبة فتم تشديد العقوبة في الفقرة الثالثة إلى الأشغال الشاقة المؤبدة إذا نتج عن الفعل ما يلي :

أ–الحاق الضرر ، ولو جزئياً ، في بناية عامة أو خاصة أو مؤسسة صناعية أو سفينة أو طائرة أو أي وسيلة نقل أو أي منشآت أخرى .

ب–تعطيل سبل الاتصالات وأنظمة الحاسوب أو اختراق شبكاتها أو التشويش عليها أو تعطيل وسائط النقل أو الحاق الضرر بها كلياً أو جزئياً.

ونلاحظ من هذه المادة في الفقرة (ب) أن المشرع قد أورد حماية لأنظمة المعلومات من الأعمال الإرهابية التي قد تمسها كتعطيلها أو اختراق الشبكة المعلوماتية أو التشويش عليها.

وبالرجوع إلى نص المادة (2) من قانون منع الإرهاب رقم (55) لسنة 2006 والتي عرفت العمل الإرهابي بأنه : (كل عمل مقصود يرتكب **بأي وسيلة** كانت يؤدي إلى...) كما نصت المادة (3/أ) من نفس القانون بأنه(مـــــع مراعاة أحكام قانون العقوبات النافذ المفعول، تحظر الأعمال الإرهابية ويعتبر في حكمها الأعمال التالية:–

أ– القيام **بأي وسيلة كانت مباشرة او غير مباشرة** ، بتقديم او جمع او تدبير الاموال بقصد استخدامها لارتكـــــــاب عمل ارهابي او مع العلم انها ستستخدم كلياً او جزئيـــاً سواء أوقع او لم يقع العمل المذكور داخل المملكة او ضد مواطنيها او مصالحها في الخارج).

نجد ومن استعراض تعريف الإرهاب طبقا للقانون المشار اليه ان المشرع يتحدث عن الوسيلة حيث وسع من نطاق الوسيلة بورود عبارة– بأي وسيلة كانت – وهنا تصبح الشبكة المعلوماتية داخل اطار الوسائل المؤدية إلي الإرهاب.

والإرهاب الالكتروني مصطلح حديث ذلك انه يعتمد علي تقنييه المعلومات من حيث وسيلة ارتكابه ومن حيث دور الفاعل وكذلك فقد استبعد وتماشيا مع القواعد العامة من عناصر الإرهاب الالكتروني البواعث والدوافع فلم يهتم التشريع بالأسباب لقيام الفاعل بارتكاب احدى جرائم الإرهاب الالكتروني فقد تكون بواعثه الشهرة أو أسباب فكرية طائفية وقد تكون بواعثه الإضرار والانتقام.

ويثور التساؤل هنا عن القانون الواجب التطبيق في حالة ارتكاب جريمة إرهابية يكون لأنظمة المعلومات ضلع فيها؟ هل هو قانون العقوبات أم قانون منع الإرهاب أم قانون جرائم أنظمة المعلومات؟

باستقراء نصوص مواد قانون جرائم أنظمة المعلومات نجد أن المادة (14) قد عالجت مشكلة تنازع القوانين وذلك بنصها على أنه:(كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية او أي نظام معلومات او اشترك او تدخل او حرض على ارتكابها يعاقب بالعقوبة المنصوص عليها في ذلك التشريع).

حيث جاء في المذكرة الإيضاحية لقانون جرائم أنظمة المعلومات انه يشمل جميع الأفعال التي تجرمها التشريعات متى ارتكبت كليا أو جزئيا بوسائل الكترونية وسواء استخدمت تلك الوسائل في ارتكاب الجريمة أو الاشتراك فيها أو التحريض عليها أو التدخل بها, كذلك فإن بعض الجرائم تم معالجتها إما في قانون العقوبات أو تشريعات خاصة، و لم يتم إدراجها في هذا القانون مما استدعى التأكيد على مراعاة معاقبة فاعلها وإن استخدم الوسائل الالكترونية في ارتكابها بدلا من الوسائل التقليدية , كما انه وباستقراء نصوص قانون منع الإرهاب نجدها لم تتطرق صراحة لمعالجة جرائم الإرهاب الإلكتروني رغم ورود عبارة بأي وسيلة كانت

فهي عباره فضفاضة تتحدث عن الوسيله بشكل عام وتم النص عليها صراحة في المادة (10) من قانون جرائم أنظمة المعلومات فالنص الخاص يقيد النص العام. ونستنتج من ذلك أن قانون جرائم أنظمة المعلومات هو الواجب التطبيق في حال ارتكاب جرائم إرهابية باستخدام أنظمة المعلومات.

المبحث الثاني

حماية أسرار الدولة

أصبحت جميع دول العالم بعد التطور التكنولوجي الكبير الذي طرأ على أنظمة المعلومات تعتمد على أجهزة الحاسب الآلي والشبكة المعلوماتية في تسيير أمورها الداخلية والخارجية, حيث أصبح الحاسب الآلي أداة ضرورية لا يمكن الاستغناء عنها من أجل تخزين وحفظ البيانات والمعلومات والوثائق الخاصة بكل دولة, كما أن هذه المعلومات ذات أهمية كبيرة فهي تمس امن الدولة و على درجة كبيرة من الخطورة كذلك فهي غير متاحة أمام الجمهور.

وهذا التطور التكنولوجي قد مد آفاق جديدة للجريمة مكنت المجرم المعلوماتي من الدخول واختراق الدعامات المحتوية على معلومات وأسرار تخص الدولة والإطلاع عليها أو العبث بها بصورة غير مشروعه من غير تصريح وهذا ما يشكل جريمة يعاقب عليها القانون, فهذه التقنية إذا ما توافرت بيد الجناة المنحرفين كنا أمام خطورة جرميه تظهر في قوالب جرميه جديدة منها جرائم التقنية المتعلقة بأمن الدولة [1].

وهذا ما جرمته المادة (11) من قانون جرائم أنظمة المعلومات وللتعرف على هذه الجريمة فقد ارتأيت إلى تقسيم هذا المبحث لمطلبين كالتالي:

المطلب الأول:ماهية جريمة الإطلاع على أسرار الدولة.

المطلب الثاني: موقف المشرع الأردني من جريمة الإطلاع على أسرار الدولة.

---

[1] الزعبي, جلال,والمناعسه,احمد , مرجع سابق.ص 258

المطلب الأول

ماهية جريمة الإطلاع على أسرار الدولة

يستطيع قراصنة الحاسب الآلي التوصل إلى المعلومات السرية والشخصية واختراق الخصوصية وسرية المعلومات بسهولة والاطلاع عليها, ويعرف سلوك التجسس بأنه فعل ايجابي قوامه الكشف واستظهار الحقائق المخفية ولكنه كشف واستظهار غير مشروع ومحل هذا السلوك المعلومات الشفهية منه والمكتوبة اياً كان نوعها إذا اتسمت بطابع السرية, فالفاعل يسعى لكشف الأسرار بغض النظر عن طبيعة هذه الأسرار أو معناها أو جهتها أو صاحبها أو قيمتها, المهم أن تتمتع تلك المعلومات بخاصية الإخفاء ومشتملات المعنى الواضح للسر,والذي لا يجوز الإطلاع عليه إلا من قبل فئة محددة محصورة وضمن قواعد وأصول مرعية تضمن حماية تلك السرية.[1]

وقد ارتأيت الى تقسيم هذا المطلب للفروع التالية :

الفرع الأول: تعريف أسرار ووثائق الدولة

الفرع الثاني: الركن المادي

الفرع الثالث: الركن المعنوي

---

[1] الزعبي, جلال,والمناعسه,احمد , مرجع سابق.ص 258

الفرع الأول

تعريف أسرار ووثائق الدولة

عرفت المادة الثانية من قانون حماية أسرار وثائق الدولة رقم (50) لسنة 1971 الأسرار والوثائق المحمية بأنها: (اية معلومات شفوية او وثيقة مكتوبة او مطبوعة او مختزلة او مطبوعة على ورق مشمع او ناسخ او اشرطة تسجيل او الصور الشمسية والافلام او المخططات او الرسوم او الخرائط او ما يشابهها والمصنفة وفق احكام هذا القانون).

ومع أتساع الاعتماد على تقنية أنظمة المعلومات تطور المفهوم التقليدي لجريمة انتهاك الحماية لإسرار ووثائق الدولة وعلى صعيد الطبيعة القانونية للركن المادي يمكن تعريف السر الإلكتروني بأنه : كل معلومة أو وثيقة محفوظة على وسيط الكتروني لا يمكن الاطلاع عليه إلا باستعمال أحدى تقنيات أنظمة المعلومات ، فالسر يوجد على نظام معلومات يحتاج إلى سلوك فني لتبيانه تمهيدا للتصرف فيه تصرفاً غير مشروع .

وقد عرفت اتفاقية لاهاي الجاسوس بأنه(كل شخص أقدم متخفياً مستتراً باحثاً عن معلومات جامعاً لها و حاولاً استقصائها جاعلاً نطاق عمله دائرة العمليات الحربية لأحد الطرفين مستهدفاً نقل المعلومات إلى الطرف الآخر.[1]

[1] الجبور . محمد عودة ,مرجع سابق , ص191

الفرع الثاني

الركن المادي

ويمكن تصور السلوك المادي لهذه الجريمة بإحدى الصورتين :

الصورة الأولى : الحصول مباشرة على الدعامة ألالكترونية الحاوية لهذا السر أو المعلومات كالحصول على ملف مخزن فيه الأسرار والوثائق المعلوماتية , وسرقة الأسرار هي الاستحواذ على الأشياء أو الوثائق أو البيانات التي يجب كتمانها حرصاً على سلامة الدولة[1]

الصورة الثانية : الدخول بصورة الكترونية إلى أنظمة تخزين تلك المعلومات والإسرار وذالك تمهيداً لارتكاب الجريمة التي سنرى صورها فيما يلي حيث إننا نبحث في الركن المادي لجريمة الكترونية مستحدثة جاءت انعكاسا لتطورات النظم المعلوماتية وتطور الفكر الإجرامي معها ،ومحاولة لبيان مقدرة النصوص التقليدية على ضبط هذه السلوكيات الجديدة وتحقيق الفاعلية العقابية [2].

ويتخذ السلوك ألجرمي المكون للركن المادي في الجريمة أحد المحاور التالية:

1- المحور الفني التقني المباشر: وهو القائم على الدخول غير المشروع لأنظمة المعالجة الإلية للمعلومات والبيانات الالكترونية والحصول على تلك البيانات والمعلومات والوثائق السرية.

[1] الجبور,محمد عودة,مرجع سابق,ص 208

[2] الزعبي, جلال,والمناعسه,احمد , مرجع سابق.ص 266

2- المحور الفني التقني غير مباشر: وهو القائم على التقاط النبضات الكهرومغناطيسية الحاملة للمعلومات والبيانات المعالجة الكترونياً وذالك بواسطة خاصة تستخدم لتلك الغاية .

وقد نصت المادة (16) من قانون حماية أسرار وثائق الدولة رقم (50) لسنة 1970 على:

(أ- من وصل إلى حيازته أو علمه إي سر من الأسرار أو المعلومات أو أية وثيقة محمية بحكم وظيفته أو كمسئول أو بعد تخليه عن وظيفته أو مسؤولية لأي سبب من الأسباب فابلغها أو أفشاها دون سبب مشروع عوقب بالإشغال الشاقة المؤقتة مدة لا تقل عن عشر سنوات .

ب- ويعاقب بالأشغال الشاقة المؤبدة إذا ابلغ ذلك لمنفعة دولة أجنبية وإذا كانت الدولة الأجنبية عدوة فتكون العقوبة الإعدام).

وبناء على ذالك لا بد من التفرقة بين الإبلاغ والإفشاء تبعاً لما جاء في نص المادة سالفة الذكر فالإبلاغ يعني نقل المعلومات والإسرار والوثائق الالكترونية المحمية من شخص إلى شخص أخر.

أما الإفشاء فهو أوسع معنى من ألإبلاغ حيث يتيح الفرصة للعامة بالاطلاع على أسرار ومعلومات الكترونية محمية من خلال الفاعل عن طريق البوح أو الإذاعة أو الكشف عما بطن أو ستر[1], والمشترط بينهما أن الفاعل يتوصل لتحقيق الإبلاغ والإفشاء بطرق الكترونية, كأن يقوم بإرسال بريد الكتروني إلى جهة ما أو ينشر تلك المعلومات والوثائق عبر صفحات الانترنت كما فعل مؤسس موقع ويكيليكس .

ولتحقيق هذا السلوك لا بد من توافر عدة عناصر:

---

[1] الجبور,محمد عودة,مرجع سابق, ص 216

أ – افتراض أن تلك المعلومات والوثائق الالكترونية موجودة تحت يد الفاعل, ويتحقق ذالك أما بارتكاب الفاعل لجريمة الحصول على تلك الأسرار المحمية سواء بطرق تقليدية أو بطرق الكترونية حديثة, وكذالك وجود تلك الأسرار والوثائق والمعلومات الالكترونية تحت يد الفاعل بحكم العمل أو بحكم علمه بها ,والحصول على جزء من السر أو على نموذج خاطئ أو ناقص منه يعتبر كالحصول عليه كاملاً.[1]

ب- أن يقوم الفاعل بإبلاغ جهة ما أو شخص ما على الأقل بتلك الأسرار آو الوثائق أو المعلومات الالكترونية سواء بمحتواها أو مضمونها.

ج- أن يتوصل الفاعل لتحقيق ذالك بطرق ووسائل الكترونية باستخدام تقنيات المعلومات والاتصالات والانترنت فإذا كان فعله مجرد سلوك تقليدي خرجنا من المفهوم الالكتروني المعلوماتي لهذه الجريمة .

د- أن يتوافر لدى الفاعل القصد ألجرمي القائم على العلم والإرادة.

الفرع الثالث

الركن المعنوي

أوضحت نصوص التجريم إلى أن حماية أسرار الدولة وكذلك حماية وثائقها ما كانت إلا لأن لها من الأهمية على أمن الدولة سواء الداخلي أو الخارجي, وأن من شأن إفشاء تلك الأسرار والوثائق والمعلومات أو الحصول عليها ممن ليس له الحق في ذلك أن يلحق الضرر بالدولة, ولذلك كان الاشتراط ليتحقق التجريم وجود قصد خاص لدى الفاعل فلا يكفي القصد العام أما

[1] الجبور,محمد عودة,مرجع سابق,ص208

القصد الخاص فيتمثل بقصد الفاعل إيقاع الضرر بالدولة والإساءة لها, ولذلك ينظر إلى انصراف نية الفاعل إلى إلحاق الضرر بالدولة وأجهزتها وكذلك شخصياتها.[1]

المطلب الثاني

موقف المشرع الأردني من جريمة الإطلاع على أسرار الدولة

نصت المادة (11) من قانون جرائم أنظمة المعلومات على انه:

(أ–كل من دخل قصدا دون تصريح أو بما يخالف أو يجاوز التصريح الي موقع الكتروني أو نظام معلومات بأي وسيلة كانت بهدف الاطلاع علي بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني يعاقب بالحبس مدة لأتقل عن أربعة أشهر وبغرامة لأتقل عن (500) خمسمائة دينار ولا تزيد علي (5000) خمسة الاف دينار "

ب– أذا كان الدخول المشار أليه في الفقرة (ا)من هذه المادة بقصد الغاء تلك البيانات أو المعلومات أو أتلافها أو تدميرها أو تعديلها أو تغيرها أو نقلها أو نسخها فيعاقب الفاعل بالإشغال الشاقة المؤقتة وبغرامة لأتقل عن (1000)ألف دينار ولا تزيد علي (5000) خمسة الإلف دينار).

تتعلق هذه المادة بالمصالح العليا للملكة ومواطنيها فالأمن الوطني والعلاقات الخارجية للمملكة وكذلك السلامة العامة وأيضا الاقتصاد الوطني كلها مصالح عليا تتعلق بسلامة جميع المقيمين

[1] الجبور ,محمد عودة,مرجع سابق, ص 204

داخل المملكة واستقرار الدولة وليس فقط مصلحة شخصية لشخص أو أكثر وبالتالي فان هذه المصالح أولي بالرعاية عن المصلحة الشخصية أو الفردية وهذا ما أدي إلي تشديد العقوبة .

وكذلك الحال بالنسبة للسلامة العامة والاقتصاد الوطني فكل ما من شانه المساس بها ممنوع العبث به أو الوصول أليه من قبل غير المصرح له وذلك حماية لتلك المصالح .

وقد شدد المشرع العقوبة في الفقرة(ب) من هذه المادة إذا كان الدخول بهدف إلغاء المعلومات أو أتلافها أو تدميرها أو تعديلها أو تغيرها أو نقلها أو نسخها وليس بهدف الاطلاع المجرد.

وقد يكون السر وصل إلي المؤتمن عن طريق وظيفته أو طبيعة عمله فقد اوجب المشرع عليه عدم إفشاء هذه الأسرار التي وصلت أليه بحكم وظيفته, فالحصول على السر من قبل شخص بمقتضى عمله الرسمي لاستخدامه أو لإبلاغه إلى سلطه مسئولة ذات صلاحية فهو حصول مشروع لا عقاب عليه , أما الإستحصال على السر فهو الوصول إليه و التمكن من إحرازه من قبل شخص لا صفة له في الحصول عليه [1].

وسوف أوضح ماهية أسرار ووثائق ألدولة من منظور القانون رقم 50 سنة 1970 ومفهومه وتطبيقه فالقانون قد جاء لحماية أمرين:

الأول: وجود أسرار ووثائق تخص مؤسسات الدولة أو أحدى هيئاتها وأن تكون هذه ألأسرار على علاقة بأمن الدولة.

الثاني: أن تكون هذه المعلومات على درجة من السرية ومجرد إفشائها يلحق الضرر بأمن الدولة الداخلي أو الخارجي وعلى ذالك فمحور الحماية ونطاق الجريمة هو السر لكن السر

---

[1] الجبور ,محمد عودة,مرجع سابق, ص208

بهذا المفهوم لا يتمتع بدرجة واحدة من الحماية فقد صنفه قانون حماية أسرار ووثائق الدولة رقم (50) لسنة 1970 إلى ثلاث أصناف وهي :

1- ألإسرار والوثائق المصنفة بدرجة سري . حيث يرى الباحثون ان أسرار ووثائق أسرار الدولة المتعلقة بدرجة سري تتعلق بخطط وتفصيلات العمليات الحربية والمعلومات والوثائق ذات العلاقة بالأمن الداخلي وكافة ألوثائق والمعلومات المتعلقة بالسياسة الخارجية والعلاقة الدولية ومنها أيضا المعلومات ألمتعلقة بوسائل ألاستخبارات والمخابرات وطرق عملها والمشتغلين بها وأيضا أي معلومة تتعلق بالأسلحة والذخائر وعتاد الجيش ومصادر قوته .

2- ألإسرار والوثائق المصنفة بدرجة سري للغاية .

وهي المتعلقة بمؤسسات الدولة أو احدي هيئاتها والتي يؤدي إفشاء أسرارها الضرر بالدولة أو إلي تحقيق منفعة لدولة أخري ومنها أية معلومات أو وثائق والقدرات الاقتصادية ومواقع مستودعات التخزين وحجم تلك الماد وكذلك تحركات القوات المسلحة والأمن العام وتعداد القوات وتسليح تلك القوات .

3- الوثائق والإسرار المصنفة بدرجة عادية .

وهي الأسرار والوثائق والمعلومات التي يؤدي إفشائها إلي إيقاع الدولة بحرج دولي ,أو يمكن ان يؤدي ذلك إلي صعوبات اقتصادية أو مالية ومنها سائر المعلومات والوثائق المتعلقة بتحقيق أو محاكمة قضائية وتلك التي يؤدي إفشائها إلي إنقاص الروح المعنوية للمواطنين كالمعلومات عن مخزون الغذاء وقت الحشد للحرب .

وبناءا على ذلك حمى المشرع الإرادة وجرم إفشاء الأسرار, ويعتبر النظام المعلوماتي في الجرائم الواقعة على أسرار الدولة والتي تمثل كافة الأسرار سواء كانت اقتصادية أو مالية أو عسكرية أو سياسية من أخطر أنواع الجرائم المعلوماتية ولذلك تعرض لها المشرع الأردني .

وأيضاً في قانون حماية أسرار ووثائق ألدولة رقم (50) لسنة 1971 وقد جاء في المادة (14)

(من دخل أو حاول الدخول إلى مكان محظور قصد الحصول على اسرار أو أشياء أو وثائق محمية أو معلومات يجب ان تبقى سرية حرصا على سلامة الدولة عوقب بالإشغال الشاقة المؤقتة وإذا حصلت هذه المحاولة لمنفعة دولة أجنبية عوقب بالإشغال الشاقة المؤبدة وإذا كانت الدولة الأجنبية عدوة فتكون العقوبة الإعدام) .

كما نصت المادة (15) من نفس القانون على انه:

(أ- من سرق أسرار أو أشياء أو وثائق أو معلومات كالتي ذكرت في المادة السابقة واستحصل عليها عوقب بالإشغال الشاقة المؤقتة لمدة لا تقل عن عشر سنوات .

ب- إذا اقترفت الجناية لمنفعة دولة أجنبية كانت العقوبة بالأشغال الشاقة المؤبدة وإذا كانت الدولة الأجنبية عدوة فتكون العقوبة الإعدام) .

واعتمادا على ما ورد في نص المادتين سالفة الذكر نجد أن المشرع قد أضفى حماية جادة لإسرار ووثائق الدولة وهذا لما لتلك الوثائق من أهمية مما جعل المشرع وصل بالعقوبة في المادة (15) بالإعدام, ألا انه يلاحظ أن المادة (14) قد ذيلت بمن دخل أو حاول الدخول ويرى الباحث أن الدخول أو محاولة الدخول تستوعب ليس فقط الدخول الجسماني بل تتعداه إلى

الدخول أو محاولة الدخول عبر شبكة المعلومات وأيضا المادة (15) حيث جاءت في الفقرة (ا) من سرق أسرار أو أشياء أو وثائق أو معلومات فالسرقة هنا تحتمل السرقة المادية وكذلك السرقة المعلوماتية خاصة وان الفقرة تتحدث عن سرقة معلومات, كما أن تعريف الأسرار والوثائق الوارد في الفقرة (2) من نفس القانون جاء موسعاً وذلك بذكر عبارة (أو ما يشابهها) حيث يدخل في ضمنها المعلومات المخزنة على الدعامات الالكترونية بالرغم من عدم وجود نص صريح يتحدث عن السرقة الالكترونية.

ويثور التساؤل هنا عن مدى انطباق نص المادتين (14و 15) من قانون حماية أسرار ووثائق الدولة عما يرتكب من جرائم مشابهه باستخدام أنظمة المعلومات؟

إن التجسس المعلوماتي والاطلاع على الأسرار المحمية والذي يتم بالوسائل التقنية الحديثة كان غائباً عن ذهن المشرع والسبب الرئيسي في ذلك هو أن هذه الجريمة في وقت إعداد قانون حماية أسرار ووثائق الدولة كانت تتم بالطرق المباشرة ,حيث لابد من الوصول إلى هذه المعلومات والوثائق من قبل احد العناصر البشرية من داخل المنشأه أو خارجها.[1]

كما أن المقصود بالدخول إلى المكان في المادة (14) هو انتقال الشخص بجسمه وحواسه إلى داخله بغض النظر عن الوسيلة التي نقلته إلى داخل ذلك المكان.[2] أي أن هذه المادة جاءت لتعالج الدخول المادي إلى الأماكن المحظورة بهدف الحصول على الأسرار والوثائق السرية وليس الدخول غير المصرح به باستخدام أنظمة المعلومات والوارد في المواد (3) و(11) من قانون جرائم أنظمة المعلومات , وفي الواقع أن محاولة تطويع نصوص هذه المواد لتشمل في طياتها جريمة التجسس على المعلومات السرية باستخدام التكنولوجيا الرقمية تتعارض مع مبدأ

[1] المومني, نهلا عبد القادر(2008), **الجرائم المعلوماتية**.ط1,عمان:دار الثقافة. ص224

[2] الجبور,محمد عودة,مرجع سابق,ص 197

جوهري وأساسي ألا وهو شرعية الجريمة والعقوبة وحظر القياس في القانون الجنائي, كما أن المادة (14) من قانون جرائم أنظمة المعلومات قد عالجت مشكلة الاختصاص حيث جاء بها أن قانون جرائم أنظمة المعلومات هو القانون المختص في حال ارتكبت إحدى الجرائم التقليدية باستخدام أنظمة المعلومات أو وقعت عليها فمن الناحية القانونية تكون المادة (11) من قانون جرائم أنظمة المعلومات هي الواجبة التطبيق.

ويري الباحث أن المشرع لم يكن موفقاً في إدراج نص المادة (11) من قانون جرائم أنظمة المعلومات وذلك للأسباب التالية:

1- إن العقوبة الواردة في المادة (14) من قانون حماية أسرار ووثائق الدولة هي عقوبة تشكل أساسيات الردع العام واكبر من العقوبة الواردة في المادة (11) ويرى الباحث أن المادة (11) جاءت كتخفيف للعقوبة إذا تم الحصول على هذه المعلومات والأسرار عن طريق النظام المعلوماتي, وبصرف النظر عن طريقة الاستحصال عليها فهي بنفس الجسامة والخطورة سواء أخذت بطرق تقليدية أو بطرق مستحدثه كما أن المادة (14) قد شددت العقوبة إذا حصلت لمنفعة دولة أجنبية أو دوله عدو على خلاف المادة (11).

2- جرمت المادة (14) من قانون حماية أسرار ووثائق الدولة الدخول أو محاولة الدخول إلى مكان محظور بقصد الحصول على هذه الأسرار أو المعلومات, فنطاق إعمال هذه المادة أوسع من نطاق إعمال المادة (11) وذلك لأنها جرمت الدخول إلى أي مكان محظور بخلاف المادة (11) التي جرمت الدخول إلى النظام المعلوماتي والموقع الالكتروني فقط, فعلى سبيل المثال لو قام احد الأشخاص بالدخول إلى منشأه عسكرية بهدف الحصول على معلومات سرية مخزنة على جهاز الحاسب الآلي الموجود داخل هذه المنشأة وتم إلقاء القبض عليه قبل

الوصول إلى الحاسوب فإن المادة (14) هنا هي الواجبة التطبيق حتى وإن كان الهدف هو النظام المعلوماتي.

3- كما أن المادة (16) من قانون حماية أسرار ووثائق الدولة قد شددت العقوبة على الموظف أو المسئول إذا أفشى أي سر من الأسرار أو المعلومات أو الوثائق المحمية أما في قانون جرائم أنظمة المعلومات فلا يوجد نص يشدد عقوبة الموظف إذا ارتكب هذه الجريمة , ففي ألفقره (ب) من المادة (11) والتي شددت العقوبة على الفاعل في حال إتلاف المعلومات أو تدميرها أو تعديلها... فهي لم تعالج الوضع القانوني للموظف أو المسئول في حال ارتكب هذه الجريمة, كما أنها تخرج من نطاق تشديد العقوبات على الموظف ومن في حكمه الواردة في نص المادة (7) من نفس القانون.

الفصل الخامس

الأحكام الإجرائية والموضوعية لجرائم أنظمة المعلومات

قد يتطلب الأمر في كثير من الأحيان ولوج البيئة المعلوماتية بحثاً عن الدليل وكشف مرتكبي الجرائم المعلوماتية لإيقاع العقوبات عليهم, وتكمن صعوبة كشف الدليل باتصاف المجرم المعلوماتي في الغالب بالذكاء والخبرة الواسعة مقارنة بنظيره المجرم التقليدي وعدم تركه لأي أثر خارجي بصورة مرئية بحيث يستطيع المجرم الالكتروني تدمير دليل الإدانة في وقت قياسي والذي من شأنه إعاقة مهمة أجهزة الاستدلال والتحقيق في الوصول إلى الدليل.[1]

وقد نظم المشرع الأردني الإجراءات الواجب إتباعها للوصول إلى الدليل والكشف عن هوية المجرمين كما بين المشرع العقوبات المفروضة عليهم في حال ارتكاب إحدى هذه الجرائم.

تقسيم :

سنتناول في هذا الفصل الإحكام الإجرائية والموضوعية الخاصة بقانون جرائم أنظمة المعلومات وذلك من خلال مناقشة مواد القانون من المادة (12) إلى (16) وسنعمل على تقسيم هذا الفصل إلى مبحثين؛ نعرض في المبحث الأول الأحكام الإجرائية الخاصة بقانون جرائم

---

[1] إبراهيم .خالد ممدوح . مرجع سابق ص79.

أنظمة المعلومات وفق ما جاءت به المواد (16,12) ثم نتناول بعد ذلك في مبحث ثاني الأحكام الموضوعية وفق ما جاءت به المواد (7,13,14,15) كالتالي:

المبحث الأول: الأحكام الإجرائية.

المبحث الثاني: الأحكام الموضوعية.

المبحث الأول

الأحكام الإجرائية

الأحكام الإجرائية هي القواعد التي تبين الأوضاع والإجراءات اللازم إتباعها أو السبيل الواجب سلوكه عند تطبيق القاعدة الموضوعية لاقتضاء الحقوق التي تقررها هذه القواعد[1]

وسنتناول في هذا المبحث أهم الأحكام الإجرائية التي جاءت بها المادة (12) من قانون جرائم أنظمة المعلومات والمتعلقة بإجراءات الضابطة العدلية كالدخول والتفتيش وضبط أجهزة الحاسب الآلي ومكوناته وكذلك الحكم بمصادرة هذه الأجهزه من قبل المحكمة , وسنوضح في المادة (16) من نفس القانون, مدى اختصاص المحاكم الأردنية في حال ارتكبت إحدى الجرائم باستخدام أنظمة المعلومات.

وبناءً على ذلك لا بد أن نستهل الحديث عن الأحكام التي جاءت بها المادة (12) حيث نصت:

(أ. مع مراعاة الشروط والاحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية ، يجوز لموظفي الضابطة العدلية ، بعد الحصول على اذن من المدعي العام المختص او من المحكمة المختصة ، الدخول إلى أي مكان تشير الدلائل الى استخدامه

[1] الزعبي.عوض أحمد (2011), مدخل الى علم القانون,عمان: اثراء للنشر والتوزيع .ص75

لارتكاب أي من الجرائم المنصوص عليها في هذا القانون ، كما يجوز لهم تفتيش الاجهزة والادوات والبرامج والانظمة والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم ، وفي جميع الاحوال على الموظف الذي قام بالتفتيش ان ينظم محضرا بذلك ويقدمه الى المدعي العام المختص.

ب. مع مراعاة الفقرة (أ) من هذه المادة ومراعاة حقوق الآخرين ذوي النية الحسنة ، وباستثناء المرخص لهم وفق أحكام قانون الاتصالات ممن لم يشتركوا بأي جريمة منصوص عليها في هذا القانون ، يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج والانظمة والوسائل المستخدمة لارتكاب أي من الجرائم المنصوص عليها او يشملها هذا القانون والاموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها.

ج. للمحكمة المختصة الحكم بمصادرة الاجهزة والادوات والوسائل وتوقيف او تعطيل عمل أي نظام معلومات او موقع الكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها او يشملها هذا القانون ومصادرة الاموال المتحصلة من تلك الجرائم والحكم بازالة المخالفة على نفقة مرتكب الجريمة).

تعالج المادة (12) أهم القواعد الإجرائية الخاصة بجرائم أنظمة المعلومات، ولعل أهم ما تعالجه هذه المادة هو التفتيش والضبط وكلاهما من المسائل المثيرة للجدل و يجب مراعاتهما بدقة حتى لا تنتهك الحريات الشخصية، ومما يجدر الإشارة إليه هو أن معظم التشريعات ومنها القانون النموذجي لجامعة الدول العربية أخذ بمبدأ "المصادرة" دون حتى تحديد الجهة المسئولة عن المصادرة أو تعريف ما هي المصادرة، كما أن الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية لعام 2001 أخذت بمبدأ التحفظ على خط سير البيانات وكذلك ضبط

ومصادرة أجهزة الكمبيوتر في حال قيام الاعتقاد لديها بوجود المعلومات والبيانات داخلها وتركت لكل دولة عضو في الاتفاقية حق اتخاذ التدابير اللازمة لذلك وفق قوانينها الداخلية،

ولذلك تم النص في مشروع قانون جرائم أنظمة المعلومات على ضرورة مراعاة التشريعات ذات العلاقة ومن بينها قانون أصول المحاكمات الجزائية الذي ينظم التفتيش والضبط والذي يعرف الضابطة العدلية واختصاصاتها, كما أن قانون الاتصالات يبين الأصول المتعلقة بتفتيش شركات الاتصالات المرخصة مما يتوجب مراعاته فيما تعلق بتلك الشركات, وكذلك تراعى التشريعات الأخرى كل منها حسب نطاق تطبيقه.

و للتعرف على الإجراءات الخاصة بجرائم أنظمة المعلومات سوف نقسم هذا المبحث إلى ثلاثة مطالب كالتالي:

المطلب الأول: التفتيش.

المطلب الثاني: الضبط والمصادرة.

المطلب الثالث: الإختصاص القضائي.

المطلب الأول

التفتيش

يعرف التفتيش بوجه عام بأنه:عبارة عن إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقاً لإجراءات قانونية محددة.[1]

ويعد التفتيش من أهم إجراءات التحقيق الابتدائي لأنه قد يؤدي إلى ضبط الأشياء المتعلقة بالجريمة إذ قد تكون أداة ارتكابها أو موضوعها أو متحصلاً عنها[2]

وقد كفل المشرع الأردني في نصوص الدستور حماية للحريات الشخصية للمواطنين وحرمة مساكنهم كما تم النص في قانون جرائم أنظمة المعلومات في المادة (12/ا)على ضرورة الحصول على إذن من المدعي العام المختص مثل الدخول إلى بيوت السكن و تفتيشها كون المدعي العام يستطيع تقدير وجود أسباب جدية تستدعي التفتيش, ولأن التفتيش من إجراءات التحقيق فلا يجوز لسلطة التحقيق مباشرة أو الإذن به إلا بمناسبة جريمة وقعت بالفعل وقامت دلائل كافيه على اتهام شخص معين بارتكابها أو مشتبهاً فيه بأنه فاعل جرم أو شريك وذلك واضح من نص المادة (81) من قانون أصول المحاكمات الجزائية حيث نصت على انه (لا يجوز دخول المنازل وتفتيشها إلا إذا كان الشخص الذي يراد دخول منزله وتفتيشه مشتبها فيه بأنه فاعل جرم او شريك او متدخل فيه او حائز أشياء تتعلق بالجرم او مخف شخصا مشتكى عليه).

ومحل التفتيش قد يكون منزلاً وهذا ما ورد في المادة السابقة وقد يكون محل التفتيش شخصاً وهذا ما نصت عليه المادة (86) من قانون أصول المحاكمات الجزائية بقولها : (1- للمدعي

---

[1] ابراهيم .خالد ممدوح(2010).فن التحقيق الجنائي في الجرائم الإلكترونية,ط1.الاسكندرية:دار الفكر الجامعي.ص182
[2] السعيد.كامل(2005). شرح قانون أصول المحاكمات الجزائية,عمان:دار الثقافه .ص445

العام ان يفتش المشتكى عليه وله ان يفتش غيره اذا اتضح من امارات قوية انه يخفي أشياء تفيد في كشف الحقيقة.

2- واذا كان المفتش انثى يجب ان يكون التفتيش بمعرفة انثى تنتدب لذلك).

أما فيما يتعلق بتفتيش شركات الاتصال (مزودوا الخدمة) فقد بين قانون الإتصالات الأصول المتبعة في تفتيش تلك الشركات حيث نصت المادة (62) على :

(الرئيس أو من يفوضه خطياً حق الدخول إلى أي مكان يشتبه بأنه يحتوي على أجهزة أو شبكات غير مرخصة أو أجهزة تستعمل للتشويش على شبكات الإتصالات أو تمارس فيها أي نشاطات مخالفة لهذا القانون أو الأنظمة الصادرة بموجبه ولهم تفتيش المكان باستثناء بيوت السكن حيث يجب الحصول على إذن من المدعي العام المختص قبل الدخول إليها وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضرا بذلك ويقدمه إلى الرئيس).

ويثور التساؤل هنا هل الإجراءات التي تحكم التفتيش في صوره السابقة هي نفسها التي تحكم نظام الحاسب الآلي ؟ وما مدى قبول نظام الحاسب الآلي للتفتيش؟

وللإجابة عن هذين السؤالين سنقسم هذا لمطلب إلى فرعين كالتالي:

الفرع الأول

مدى قابلية نظام الحاسب الآلي للتفتيش

إن تفتيش نظم الحواسيب هو تفتيش للفضاء الإفتراضي وأوعية التخزين وتفتيش البيانات التي يحفظها جهاز الكمبيوتر إذا كان مزوداً بذاكرة الكترونية تحفظ العمليات المنجزة من خلاله ,كما أن تفتش نظم الحواسيب قد يكون له عواقب قانونية أهمها بطلان الإجراءات إذا كانت خارج نطاق أمر التفتيش.

أما الدخول غير المصرح به وفق ما جاءت به المادة (3) من قانون جرائم أنظمة المعلومات من أجل البحث والتنقيب في البيانات والبرامج المستخدمة أو في الملفات المخزنة عما قد يتصل بجريمة وقعت فهو إجراء جائز قانوناً – بعد الحصول على اذن من المدعي العام المختص او المحكمة المختصه– ولو لم ينص عليه صراحة باعتباره يدخل في نطاق التفتيش بمعناه القانوني ويندرج تحت مفهومه لما تقتضيه مصلحة وظروف التحقيق والكشف عن الحقيقة في الجرائم المعلوماتية[1]

ومحل التفتيش في الجرائم المعلوماتية هو جهاز الكمبيوتر والأجهزة المتصلة به عن طريق الشبكة وهذا يعني أن التفتيش سوف ينصب على المكونات التالية:

ا– تفتيش المكونات المادية و المنطقية (الغير ملموسة)لجهاز الحاسوب.

جاء في نص المادة (12/أ) من قانون جرائم أنظمة المعلومات (كما يجوز لهم تفتيش الأجهزة والأدوات والأنظمة والوسائل التي تشير الدلائل إلى استخدامها لإرتكاب أي من تلك الجرائم).

ففي الجريمة التقليدية ينصب التفتيش على شخص المتهم أو غير المتهم وكذلك على مسكن المتهم وما في حكمه, ولكن في الجريمة المعلوماتية فإن محل التفتيش هي مكونات الحاسب الآلي سواء أكانت مادية أم غير مادية.

---

[1] ابراهيم .خالد ممدوح,مرجع سابق,ص194

وتتمثل المكونات المادية للحاسب الآلي في:[1]

أجهزة إدخال البيانات data entry devices

1 لوحة المفاتيح key board

2 الفأرة mouse

3 المشغلات drivers

–مشغل الأقراص الصلبة hard disk

–مشغل الأقراص المرنة floppy disk drive

–مشغل الأقراص المدمجة CD-ROM

4 الماسح الضوئي scanner

أجهزة إخراج المعلومات information output devices

1 الشاشة monitor

2 الطابعات printers

3 عارض البيانات data show

4 مكبرات الصوت speakers

وحدات الإدخال و الإخراج input output units

---

[1] الهيتي.محمد حماد(2006),**جرائم الحاسوب**,ط1.عمان:دار المناهج للنشر والتوزيع,ص34 وما بعدها

1 وحدة الذاكرة الرئيسية Main memory (ram)

2 وحدة المعالجة المركزية central Processing unit(CPU)

3 وسائط التخزين الخارجية وتشمل الأقراص الليزرية CD والذاكرة الضوئية flash ram

4 المودم Modem

إن حكم تفتيش المكونات المادية للحاسب الآلي يتوقف على طبيعة المكان الموجودة فيه تلك المكنونات وهل هو من الأماكن العامة أو الأماكن الخاصة حيث للمكان أهمية خاصة في مجال التفتيش[1], فإذا كانت موجودة في مكان خاص كمنزل المتهم فلا يجوز تفتيشها إلا في الحالات التي يجوز تفتيش المنازل و بنفس الضمانات والإجراءات المقررة في المادة (81) من قانون أصول المحاكمات الجزائية .

أما لو وجد شخص يحمل مكونات الكمبيوتر المادية كالأقراص المضغوطة وكان يخفيها معه أو حائزاً لها في مكان ما من الأماكن العامة فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في المادة (86) من قانون أصول المحاكمات الجزائية.

أما عن تفتيش الحاسبات الآلية التي تقع في أماكن عامة كالحاسبات الشخصية (الآبتوب) والتي يحملها الشخص خارج منزله, فإن تفتيش أنظمتها لا يكون جائزاً إلى في الأحوال التي يجيز

[1] ابراهيم .خالد ممدوح,مرجع سابق,ص196

فيها القانون تفتيش الأشخاص باعتبار أن تفتيش الشخص يشمل ذاته وكل ما في حوزته وقت هذا التفتيش وسواء كان مملوكاً لغيره أم لا.[1]

أما المكونات المعنوية (الغير ملموسة) للحاسب الآلي فإنها تنقسم إلى الكيانات المنطقية الأساسية أو برامج النظام أو برامج التطبيقات سابقة التجهيز وبرامج التطبيقات طبقاً لاحتياجات المستخدم[2]

كما إن تفتيش المكونات المعنوية الغير ملموسة للحاسب الآلي قد أثار خلافاً كبيراً في الفقه بشأن جواز تفتيشها , فذهب رأي إلى أنه متى كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الجريمة فإن هذا المفهوم يمتد حتى يشمل البيانات الإلكترونية بمختلف أشكالها , وعلى العكس من ذلك فهناك من يرى بأن هذا المفهوم المادي لا ينطبق على بيانات الحاسب الآلي غير الملموسة إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية.[3]

وحسناً فعل المشرع الأردني حيث حسم النزاع في المادة (12/أ)من قانون جرائم أنظمة المعلومات حيث أجازت تفتيش البرامج والأنظمة, وبالرجوع إلى المادة (2) من نفس القانون التي عرفت البرنامج بأنه (مجموعة من الأوامر والتعليمات الفنية المعدة لانجاز مهمة قابلة للتنفيذ باستخدام أنظمة المعلومات) كما عرفت نظام المعلومات بأنه(مجموعة البرامج والادوات المعدة لانشاء البيانات او المعلومات الكترونيا ، او ارسالها او تسلمها او معالجتها او تخزينها او ادارتها).و بما أن البرامج و النظام هم عبارة عن أوامر وتعليمات فنية أو

---

[1] ابراهيم .خالد ممدوح,مرجع سابق,ص207
[2] حجازي,عبد الفتاح بيومي(2007).مبادي الإجراءات الجنائية في جرائم الكمبيوتر و الانترنت.مصر:دار الكتب القانونية.ص389
[3] يوسف ،امير فرج ,مرجع سابق. .ص224

معلومات الكترونية غير ملموسة فنستنتج من ذلك أن التفتيش يمتد ليشمل المكونات المنطقية للحاسب الآلي سنداً للمادة (12/أ) من قانون جرائم أنظمة المعلومات.

الفرع الثاني

مدى خضوع شبكات الحاسب الآلي للتفتيش

الاحتمال الأول: في حال كان حاسب المتهم متصلاً بحاسب أو نهاية طرفية موجودة في مكان آخر داخل الدولة.

يثار التساؤل حول مدى إمكانية امتداد الحق في التفتيش إذا تبين أن الكمبيوتر أو النهاية الطرفية في منزل المتهم متصلة بجهاز أو نهاية طرفية في مكان آخر مملوك لشخص آخر خلاف المتهم؟

يرى الفقه الألماني إمكانية امتداد التفتيش إلى سجلات البيانات التي تكون في مكان آخر استناداً إلى مقتضيات القسم(103)من قانون الإجراءات الجنائية الألماني[1]

كما نص قانون تحقيق الجنايات البلجيكي في المادة (88)على أنه (إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي أو في أي جزء منه فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي) [2]

أما قانون جرائم أنظمة المعلومات فلا يوجد به نص صريح يجيز الدخول وامتداد التفتيش إلى النظام المعلوماتي الموجود في مكان آخر غير مكان المتهم كما فعل المشرع البلجيكي.

---

[1] ابراهيم .خالد ممدوح,مرجع سابق,ص203

1ابراهيم .خالد ممدوح,مرجع سابق,ص203

لكن المادة (12/أ) من نفس القانون أجازت بشكل عام دخول موظفي الظابطه العدلية –بعد الحصول على إذن– إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب جريمة معلوماتية كما أجازت هذه المادة تفتيش الوسائل التي تشير الدلائل في استخدامها لارتكاب الجريمة.

ومن هنا نرى أن النص جاء موسع وذلك بذكر عبارة (أي مكان) والتي تشمل أيضاً بيوت السكن, ومع مراعاة التشريعات النافذة و منها قانون أصول المحاكمات الجزائية نجد أن المادة (82) والتي تنص على انه: (مع مراعاة الأحكام السابقة يحق للمدعي العام أن يقوم بالتحريات في جميع الأمكنة التي يحتمل وجود أشياء او أشخاص فيها يساعد اكتشافها او اكتشافهم على ظهور الحقيقة).وقد أعطت المدعي العام صلاحية التحري في جميع الأمكنة المشتبه بها وكذلك جاءت عبارة (أشياء) وهو مصطلح واسع يدخل في طياته الحاسب الآلي ومكوناته وتوابعه و نستنتج من ذلك و بناءاً على النصوص السابقة أن التفتيش ممكن أن يمتد ليشمل جهاز حاسوب موجود في مكان آخر مرتبط بنهاية طرفية متصلة بجهاز حاسوب المتهم.

الإحتمال الثاني: اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة.

من المتصور طبقاً لهذا الفرض أن يقوم مرتكبو الجريمة المعلوماتية بتخزين البيانات والبرامج التي تستخدم في ارتكاب الجريمة على دعامات تقنية لحواسيب موجودة خارج حدود الدولة

عن طريق شبكات الاتصال العالمية (الإنترنت) بهدف عرقلة الجهات المختصة في جمع الأدلة.[1]

وهذه من المشاكل التي تواجه الضابطة العدلية في جمع الأدلة والتحقيقات حالة امتداد التفتيش إلى خارج الإقليم الجغرافي للدولة إذ يصبح البحث عن الدليل أمراً في غاية الصعوبة ، إن لم يكن مستحيلاً أحياناً ، على اعتبار أن التفتيش في هذه البيئة الافتراضية يتطلب أن يتم خارج حدود الدول وفي نطاق دولة أخرى وقد يتعذر القيام به بسبب تمسك كل دولة بسيادتها, لذا فإن جانب من الفقه يرى أن التفتيش الإلكتروني العابر للحدود الجغرافية للدول يجب أن يتم في إطار اتفاقيات تعاون خاصة ثنائية أو دولية تجيز هذا الامتداد حيث لا يجوز القيام بذلك التفتيش العابر للحدود في ظل غياب تلك الاتفاقيات أو على الأقل الحصول على إذن الدولة الأخرى.[2]

المطلب الثاني

الضبط والمصادرة

[1] حجازي,عبد الفتاح بيومي,مرجع سابق,ص382

[2] ابراهيم .خالد ممدوح,مرجع سابق,ص206

يعني ضبط الأشياء وضع اليد عليها والمحافظة عليها من قبل السلطات المختصة بالتحقيق والغالب أن تكون الأشياء المضبوطة حصيلة أو نتيجة التفتيش الذي قام به المدعي العام أو من أنابه[1]

والحقيقة أن الضبط بطبيعته والتنظيم القانوني له لا يرد سوى على الأشياء أما الأشخاص فليسو محلاً للضبط بالمعنى الدقيق أو المفهوم ويستوي في ذلك ضبط المنقول والعقار وقد يكون المضبوط مملوكاً للمتهم أو لغيره[2]

و الضبط بحسب الأصل لا يرد إلا على أشياء مادية فلا يوجد صعوبة بضبط أدلة الجريمة الواقعة على المكونات المادية للحاسوب, وكذلك لا صعوبة أيضاً في ضبط الدعامة المادية للبرنامج أو الحاسوب وملحقاته.

ولكن تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في إتلاف النظام المعلوماتي مثل برامج الفيروس والديدان وفي ضبط بيانات الحاسوب لعدم وجود أي دليل مرئي في هذه الحالات ولسهولة تدمير الدليل في ثواني معدودة[3].

ويثور التساؤل هنا عن مدى إمكانية ضبط البيانات المعنوية والغير ملموسة للحاسب الآلي؟

---

[1] السعيد,كامل,مرجع سابق,ص467

[2] حجازي,عبد الفتاح بيومي,مرجع سابق,ص394

[3] ابراهيم .خالد ممدوح,مرجع سابق,ص274

أعطت المادة (87) من قانون أصول المحاكمات الجزائية الصلاحية للمدعي العام بضبط جميع الأشياء التي يراها ضرورية لإظهار الحقيقة, حيث نصت هذه المادة على (يصطحب المدعي العام كاتبه ويضبط او يأمر بضبط جميع الاشياء التي يراها ضرورية لاظهار الحقيقة ونظم بها محضرا ويعنى بحفظها وفقا لأحكام الفقرة الاولى من المادة (35).

كما نصت المادة (1/34) من نفس القانون على (1- اذا وجد في مسكن المشتكى عليه أوراق او أشياء تؤيد التهمة او البراءة فعلى المدعي العام ان يضبطها وينظم بها محضرا).

ونرى من هذين النصين أن المشرع قد توسع في معنى الضبط عندما ذكر عبارة (وأشياء)

وقد ذهب رأي من الفقه عن البحث عما إذا كانت كلمة أشياء تشمل البيانات المعنوية لمكونات الحاسب الآلي فذهب إلى أن النظرة في ذلك يجب أن تستند إلى الواقع العملي الذي يتطلب أن يقع الضبط على بيانات الحاسب الآلي إذا اتخذت شكلا مادياً, وكذلك نجد أن القسم (94) من قانون الإجراءات الألمانية ينص على أن (الأدلة المضبوطة يجب أن تكون ملموسة) ويسير قانون العقوبات في رومانيا على ذات النهج[1]

ويرى الباحث ان الضبط المنصوص عليه في المادتين (87,34) من قانون أصول المحاكمات الجزائية يمكن أن ينطبق فقط على ضبط الأشياء المادية بالنسبة لمكونات الحاسوب, ويشمل أيضا البيانات التي تحتويها دعامة مادية كالأقراص الصلبة و المضغوطة أما البيانات ككيان معنوي غير ملموس فإنها لا تكون محلاً للضبط وفق هاتين المادتين.

وقد عالج المشرع الأردني مسالة ضبط المكونات المعنوية للحاسب الآلي حيث نصت المادة (12) في البند (ب) من قانون جرائم أنظمة المعلومات على (مع مراعاة الفقرة (أ) من هذه

---

[1] ابراهيم .خالد ممدوح,مرجع سابق,ص198

المادة ومراعاة حقوق الآخرين ذوي النية الحسنة ، وباستثناء المرخص لهم وفق أحكام قانون الاتصالات ممن لم يشتركوا بأي جريمة منصوص عليها في هذا القانون ، يجوز لموظفي الضابطة العدلية ضبط الاجهزة والادوات **والبرامج والانظمة** والوسائل المستخدمة لارتكاب أي من الجرائم المنصوص عليها او يشملها هذا القانون والاموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها).

وباستقراء الفقرة (ب)نجد أن المشرع أجاز صراحة لموظفي الضابطة العدلية ضبط المكونات المعنوية بالإضافة إلى المكونات المادية للحاسب الآلي وهذا واضح من ذكر عبارة (والبرامج والأنظمة) حيث تم تعريفها سابقاً, ونستنتج من هنا أن كلا التفتيش و الضبط وحسب ما جاءت به المادة (12) فإنه يقع على المكونات المادية والمنطقية للحاسب الآلي.

و كذلك نصت ايضاً على إمكانية التحفظ على المعلومات والبيانات المتعلقة بإرتكاب الجريمة ,حيث تتم عملية التحفظ على الأدلة داخل جهاز الحاسوب بأساليب متعددة, وتكمن أقوى مظاهرها في عمليات حجز الحاسوب على الدليل الموضوع فيه ,أما بالنسبة لعملية حفظ الأدلة في العالم الرقمي (الإنترنت) فإنه يتطلب من الخبير التقني القيام برصد موقع الإنترنت أو المعلومات التي تشير إلى الجريمة كما لو كانت مثلا من جرائم الذم و القدح و التحقير في غرف المحادثة ومواقع التواصل الاجتماعي, ففي مثل هذه الحالة يتم اللجوء إلى ذاكرة الخادم الذي يتولى ربط هذه الغرف عبر العالم الرقمي , كذلك فيمكن اللجوء إلى اخرج الأدلة من إطار الحاسوب والعالم الرقمي إلى العالم المادي بحيث يتم التعامل معها كمخرجات يقبلها القضاء كأدلة كاملة في الجريمة تساعد في الإدانة أو البراءة.

أما فيما يتعلق بالضبط المتعلق بشركات الإتصال (مزودوا الخدمة) فقد جعله المشرع من اختصاص موظفو هيئة تنظيم قطاع الاتصالات على اعتبار أنهم من رجال الضابطة العدلية, كما اشترط التقيد بالشروط المنصوص عليها بقانون أصول المحاكمات الجزائية حيث نصت المادة (63/أ) من قانون الاتصالات على انه (أ- يعتبر موظفو الهيئة المفوضون بضبط المخالفات من رجال الضابطة العدلية ويعمل بالضبوط المنظمة من قبلهم إلى أن يثبت عكسها شريطة التقيد بشروط الضبط المنصوص عليها في قانون أصول المحاكمات الجزائية المعمول بها).

أما البند (ج) من المادة (12) من قانون جرائم أنظمة المعلومات والذي ينص على:

(للمحكمة المختصة الحكم بمصادرة الاجهزة والادوات والوسائل وتوقيف او تعطيل عمل أي نظام معلومات او موقع الكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها او يشملها هذا القانون ومصادرة الاموال المتحصلة من تلك الجرائم والحكم بازالة المخالفة على نفقة مرتكب الجريمة).

وهذا النص جعل الحكم بالمصادرة من صلاحيات المحكمة وهذا ما تأخذ به جميع التشريعات الأردنية والتشريعات المقارنة وللمحكمة أن تصادر أجهزة تم ضبطها من قبل الضابطة العدلية أو ما لم يتم ضبطه ابتداء وفقاً للقواعد الخاصة بالمصادرة في التشريعات ذات العلاقة, حيث نصت المادة (30) من قانون العقوبات على(مع مراعاة حقوق الغير ذي النية الحسنة ، يجوز مصادرة جميع الاشياء التي حصلت نتيجة لجناية أو جنحة مقصودة أو التي استعملت في ارتكابها أو كانت معدة لاقترافها . أما في الجنحة غير المقصودة أو في المخالفة فلا يجوز مصادرة هذه الاشياء الا اذا ورد في القانون نص على ذلك).

كما نصت المادة (31) من نفس القانون على (يصادر من الأشياء ما كان صنعه أو اقتناؤه أو بيعه أو استعماله غير مشروع وإن لم يكن ملكاً للمتهم أو لم تفض الملاحقة الى حكم).

حيث أجازت المادة (30)مصادرة جميع الأشياء التي حصلت نتيجة جناية أو جنحه وعليه يتم مصادرة مكونات الحاسب الآلي التي استخدمت في ارتكاب الجريمة أو التي كانت تعد لاقترافها, كما أجازت المادة (31) من نفس القانون مصادرة الأشياء التي يكون صنعها أو اقتناؤها أو بيعها أو استعمالها غير مشروع كمصادرة آله تستخدم في تزوير النقود موصلة في الحاسب الآلي, كما أتاح البند (ج) أيضا للمحكمة المختصة بإمكانية توقيف أو تعطيل عمل أي نظام معلوماتي أو موقع الكتروني يستخدم لارتكاب الجرائم المعلوماتية كذلك فتصادر أيضاً الأموال المتحصلة منها كارتكاب جريمة سرقة لأحد البنوك باستخدام أنظمة المعلومات .

المطلب الثالث

الإختصاص القضائي

عالجت المادة (16) من قانون جرائم أنظمة المعلومات موضوع الإختصاص القضائي في حال ارتكبت إحدى الجرائم باستخدام أنظمة المعلومات حيث نصت على :

(يجوز اقامة دعوى الحق العام والحق الشخصي على المشتكى عليه امام القضاء الاردني اذا ارتكبت أي من الجرائم المنصوص عليها في هذا القانون باستخدام انظمة معلومات داخل المملكة او الحقت اضرارا باي من مصالحها او باحد المقيمين فيها او ترتبت اثار الجريمة فيها ، كليا او جزئيا ، او ارتكبت من احد الاشخاص المقيمين فيها).

تهدف المادة (16)إلى معالجة الاختصاص القضائي فيما تعلق بجرائم أنظمة المعلومات في الوقت الذي يعتبر مبدأ الإقليمية هو المبدأ المهيمن على تطبيق القانون الجنائي من حيث المكان الأمر الذي لا يستقيم بالنسبة لجرائم أنظمة المعلومات, ولذلك السبب وحماية لمصالح الدولة وهيبتها وحماية لمصالح رعاياها، فقد تم النص على الاختصاص القضائي للمحاكم الأردنية متى تمت الجريمة باستخدام أنظمة معلومات داخل المملكة أو ألحقت اضراراً بأي من مصالحها أو بأحد المقيمين فيها أو ترتبت آثار الجريمة فيها أو ارتكبت من أحد الأشخاص المقيمين فيها, والغاية من وضع هذا النص هو منع اللجوء من قبل الفاعل إلى اختصاصات قضائية أخرى لارتكاب جريمة تستهدف مصالح داخل المملكة بغية التملص من العقاب، فقد يقرر أي شخص استخدام أنظمة معلومات أو مواقع الكترونية خارج المملكة لتنفيذ جرائم بحق مواطنيها أو المقيمين فيها كنوع من التحايل على القانون أو للإفلات من العقاب، وهذه المادة تحول دون ذلك.

فالجريمة المعلوماتية قد ترتكب في دولة معينه ويكون أثرها في إقليم الدولة التي ارتكبت فيها وقد يمتد هذا الأثر ليتم في دولة أخرى , ويمكن أن تصل إلى عدد غير محدد من الدول[1]

وعالجت المادة (5) في الفقرة (4) من قانون أصول المحاكمات الجزائية موضوع اختصاص القضاء الأردني في حال ارتكبت الجريمة بوسائل الكترونية من خارج المملكة, حيث نصت على انه (يجوز اقامة دعوى الحق العام على المشتكى عليه امام القضاء الاردني اذا ارتكبت الجريمة بوسائل الكترونية خارج المملكة وترتبت اثارها فيها ، كليا او جزئيا ، او على أي من مواطنيها).

ونجد أن نطاق تطبيق المادة (16) من قانون جرائم أنظمه المعلومات أوسع منه من المادة (5) من قانون أصول المحاكمات الجزائية حيث شملت الأولى المقيمين في المملكة من غير الأردنيين.

أما فيما يتعلق بإقامة دعوى الحق الشخصي فقد نصت عليها المادة (16) بقولها(يجوز اقامة دعوى الحق العام والحق الشخصي على المشتكى عليه..) ويقصد بدعوى الحق الشخصي بالمعنى الضيق: هي الدعوى التي يقيمها المتضرر من جريمة أمام القضاء الجزائي تبعاً لدعوى الحق العام بغية الحصول على تعويض عن الضرر الذي لحقه من تلك الجريمة[2].

المبحث الثاني

[1] الحسيناوي,علي جبار,مرجع سابق,34

[2] السعيد,كامل,مرجع سابق,ص211

الأحكام الموضوعية

الأحكام الموضوعية هي التي تضع تنظيماً وقواعد موضوعية للروابط الاجتماعية فتبين الحقوق والواجبات المختلفة وتضمن الجزاء المادي الذي يوقع على من يخالف أحكامها كقواعد قانون العقوبات وغيره[1].

وسوف نتناول في هذا المبحث الأحكام الموضوعية التي جاء بها قانون جرائم أنظمة المعلومات رقم (30) لسنة 2010 وبيان الظروف المشدد للعقوبة والأحكام الخاصة بالموظف وعقوبة كل من المشترك والمحرض والمتدخل في الجريمة المعلوماتية, وعليه ارتأيت الى تقسيم هذا المبحث إلى مطلبين كالتالي :

المطلب الأول : تشديد العقوبة.

المطلب الثاني : عقوبة الشريك والمتدخل والمحرض.

المطلب الأول

[1] الزعبي.عوض أحمد,مرجع سابق,ص75

تشديد العقوبة

جاءت المادة (3/ب) من قانون جرائم أنظمة المعلومات بأحكام خاصة تشدد من العقوبة إذا كان هدف الجاني من الدخول غير المصرح به القيام بأحد الأفعال الواردة في هذا البند, حيث نصت على انه : (ب. اذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة بهدف الغاء او حذف او اضافة او تدمير او افشاء او اتلاف او حجب او تعديل او تغيير او نقل او نسخ بيانات او معلومات او توقيف او تعطيل عمل نظام معلومات او تغيير موقع الكتروني او الغائه او اتلافه او تعديل محتوياته او اشغاله او انتحال صفته او انتحال شخصية مالكه

فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة او بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) الف دينار او بكلتا هاتين العقوبتين).

ويتضمن البند (ب) من المادة (3) عقوبة مشددة لجريمة الدخول غير المصرح به المنصوص عليها في الفقرة (أ) من ذات المادة، حيث أن الدخول بحد ذاته جريمة معاقب عليها، فإذا كان الدخول بهدف ارتكاب أي من الأفعال أو تحقيق أي من النتائج التي ينص عليها البند (ب) موضوع البحث، فتشدد العقوبة بحق الفاعل حيث تصبح كالتالي:

الحبس (مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة) بدلا من (مدة لا تقل عن اسبوع ولا تزيد على ثلاثة اشهر) .

كما أن الغرامة قد أصبحت (لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار) بدلا من (لا تقل عن (100) مائة دينار ولا تزيد على (200) مائتي دينار).

أما فيما يتعلق في المادة (6) من نفس القانون فقد جاءت الفقرة (أ) منها بأحكام موضوعية تجرم فعل الحصول العمدي دون تصريح على البيانات والمعلومات المتعلقة بالمعاملات المالية والمصرفية وبطاقات الائتمان وجاء تشديد العقوبة في الفقرة (ب) حيث نصت على:

(ب. كل من استخدم عن طريق الشبكة المعلوماتية او أي نظام معلومات قصدا دون سبب مشروع بيانات او معلومات تتعلق ببطاقات الائتمان او بالبيانات او المعلومات التي تستخدم في تنفيذ المعاملات المالية او المصرفية الالكترونية للحصول لنفسه او لغيره على بيانات او معلومات او اموال او خدمات تخص الاخرين يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن (1000) الف دينار ولا تزيد على (5000) خمسة الاف دينار).

والسبب في تشديد العقوبة هنا لأن الفاعل لم يقف على مجرد الحصول على البيانات الخاصة بالمعاملات المالية وبطاقة الائتمان كما هو وارد في ألفقره (أ) بل تعدى ذلك في استخدام تلك المعلومات للحصول لنفسه أو لغيره على بيانات أو أموال أو خدمات تخص الآخرين بقصد الحصول على منفعة غير شرعية ,ويطلق على مثل هذا الفعل السرقة الإلكترونية أو الاحتيال الإلكتروني, وتكمن خطورة مثل هذا الفعل في سهولة ارتكاب الجريمة وصعوبة اكتشافها وبالتالي تم تشديد عقوبتها حماية للنظام المالي والمصرفي الالكتروني والمعاملات الالكترونية وحقوق المتعاملين بها.

وتشدد العقوبة بحق الفاعل حيث تصبح كالتالي :

الحبس (مدة لا تقل عن سنة) بدلاً من (الحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين) أما الغرامة فتصبح (لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار.) بدلاً من (لا تقل عن (500) خمسمائة دينار ولا تزيد على (2000) ألفي دينار)

وقد جاءت المادة(11) في ألفقره (ب) منها لتشدد العقوبة على الفاعل حيث نصت على (ب. اذا كان الدخول المشار اليه في الفقرة (أ) من هذه المادة بقصد الغاء تلك البيانات او المعلومات او اتلافها او تدميرها او تعديلها او تغييرها او نقلها او نسخها ، فيعاقب الفاعل بالاشغال الشاقة المؤقتة وبغرامة لا تقل عن (1000) الف دينار ولا تزيد على (5000) خمسة الاف دينار.)ويأتي التجريم في الفقرة (أ) من هذه المادة اذا كان هدف الجاني من الدخول مجرد الإطلاع ويكون التشديد إذا تجاوز الجاني بأفعاله مجرد الإطلاع على البيانات والمعلومات الغير متاحه للجمهور وذلك بإلغاءها أو اتلافها أوتعديلها ... فالمادة (11) تتعلق بالمصالح العليا للمملكة ومواطنيها، فالأمن الوطني والعلاقات الخارجية للمملكة والسلامة العامة والاقتصاد الوطني جميعها مصالح عليا تتعلق بسلامة جميع المقيمين داخل المملكة واستقرار الدولة وليس مجرد مصلحة شخصية لشخص أو أكثر وبالتالي فإن هذه المصالح أولى بالرعاية من المصالح الفردية مما استدعى تشديد العقوبة, ومن الأمثلة على المصالح التي تحميها هذه المادة كل ما يتعلق بالخدمات العامة كالمياه والهاتف والكهرباء والدفاع المدني والبنوك إضافة للهيئات الدبلوماسية والرسمية وغيرها.

وإذا ارتكب الجاني احد الأفعال المنصوص عليها في البند (ب) فتشدد العقوبة بحقه حيث تصبح كالتالي:

الأشغال الشاقة المؤقتة بدلاُ من بالحبس مدة لا تقل عن أربعة أشهر

أما الغرامة فتصبح لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار بدلا من الغرامة التي لا تقل عن (500) خمسمائة دينار ولا تزيد على (5000) خمسة آلاف دينار.

ويثور التساؤل هنا في حال قيام أحد المشتركين في الجريمة بإخبار السلطات بوجود جريمة (مؤامرة) تمس أمن الدولة ترتكب باستخدام أنظمة المعلومات فهل تخفف العقوبة بحقه؟

نصت المادة (109) من قانون العقوبات على انه:

(1- يعفى من العقوبة من اشترك في مؤامرة على أمن الدولة وأخبر السلطة بها قبل البدء بأي فعل مهيء للتنفيذ.

2- اذا ارتكب فعل كهذا أو بدء به لا يكون العذر إلا مخففاً.

3- يستفيد من العذر المخفف ، المتهم الذي أخبر السلطة بمؤامرة أو بجريمة أخرى على أمن الدولة قبل إتمامها أو أتاح القبض – ولو بعد مباشرة الملاحقات – على المتهمين الآخرين أو على الذين يعرف مختبأهم.

4- لا تطبق أحكام هذه المادة على المحرض).

ويري الباحث أن الجرائم التي تقع على أمن الدولة وسلامتها بواسطة أنظمة المعلومات لا تقل خطورة عن الجرائم المماثلة التي تقع بطرق تقليدية بحيث يستطيع الجناة الكشف عن معلومات خطيرة تمس الأمن الوطني أو تكوين موقع الكتروني ونشر هذه المعلومات أو دس الدسائس بين صفوف المواطنين وهذا ما يزعزع الأمن والاستقرار في الدولة, كذلك فالغاية التي توخاها المشرع من الأعذار المخففة الخاصة والواردة في المادة (109) تهدف إلى تشجيع الكشف عن الجرائم التي تحاط بسرية وكتمان وحسن تنظيم وتسهيلاً لإعمال سلطات الضبط والتحقيق فهي

في الحقيقة تعتبر مكافأة من المشرع إلى المتورط في طريق الإجرام بتخفيف العقوبة عليه عن الجريمة التي تورط فيها عن طريق البوح عن المتورطين معه فيها[1].

ويرى الباحث أن المادة سالفة الذكر تنطبق على الجرائم التي تمس أمن الدولة والتي أداتها أنظمة المعلومات.

الفرع الأول

الموظف ومن في حكمة

نصت المادة (7) من قانون جرائم أنظمة المعلومات رقم 30 لسنة 2010 على انه:

(تضاعف العقوبة علي الجرائم المنصوص عليها في الماد من (3) إلي (6) من هذا القانون بحق كل من قام بارتكاب أي منها أثناء تأدية وظيفته أو عمله أو باستغلال أي منهما).

وبذلك فالمادة سالفة الذكر تعالج الجرائم التي يرتكبها الموظف العام أو من في حكمه وقد جاء في المذكرة الإيضاحية لمشروع القانون أمثلة لهؤلاء من أمثال المستشار , العامل , المقاول, وغيرهم وبذلك خرج مفهوم الموظف العام عما هو مقصود ومعني في القانون الإداري وإنما توسع المشرع وذلك بقوله كلمة وظيفته وهي بالتالي تعني كل من يعمل لدى شخص أو مستخدم لدى أي شركة أو مؤسسة, وبهذا فالعقوبة تشمل الموظف العام أو الموظف الخاص دون تفرقة, وفلسفة المشرع في التوسع في مفهوم الموظف هي لان من يستغل عمله لدى أي جهة لارتكاب وتوجيه تلك الأفعال المجرمة إلى الجهة التي يعمل لديها أو من يتعامل معهم

[1] الجبور,محمد عودة,مرجع سابق,ص502

بحكم عمله فهم مؤتمنون على مصالح صاحب العمل وعلى أسرار ومعلومات وأموال وحقوق المتعاملين معهم ممن اتكلوا على أمانتهم, فان ارتكاب أي من الجرائم المنصوص عليها في المواد من (3– 6) من قانون جرائم أنظمة المعلومات أسهل بالنسبة لهؤلاء لأنهم تمكنوا بحكم عملهم من الوصول والحصول على المعلومات بيسر, وأيضا فان هؤلاء يعلمون نقاط الضعف والقوة ومدى أهمية تلك البيانات والمعلومات, كما أن الدخول غير المشروع لنظام المعلومات والشبكة المعلوماتية لصاحب العمل ومن يتعاملون معه من موظفين وعملاء ومؤسسات وغيرهم أسهل وأيسر بالنسبة لهؤلاء مما هو للغير.

ألا أن السؤال الذي يطرح نفسه وبقوة هو ماهية التكييف القانوني لتشديد العقوبة التي جاءت بها المادة (7) هل هي جريمة اختلاس أم جريمة إساءة ائتمان؟

وللإجابة علي ذلك السؤال يجب أن نشير إلى مفهوم القصد الجرمي وهي تبعا لإرادة النتيجة التي قد تأتي مباشرة أو بإرادة نتيجة بسيطة في الحالات التي يستلزم القانون أحداث نتيجتين احدهما بسيطة الأخرى جسيمة[1]

فالقصد المباشر يكون عندما يوجه الجاني إرادته بصورة حاسمة نحو أحداث النتيجة ويتحقق ذلك بارتكاب الفعل ضد الحق.

وهناك القصد الاحتمالي وتعد الجريمة مقصودة وان تجاوزت النتيجة قصد الفاعل أذا كان قد توقع حصولها فقبل المخاطرة, وهناك القصد المتعدي وقد يلقي القانون عبء نتائج غير مقصودة على الفاعل ولو لم يقبلها.

---

[1] الجبور ,محمد عوده,مرجع سابق,ص252

ويجب إن يكون هناك تسليم للمال إلي الجاني حتى تتوافر الجريمة وفي هذا تفترق عن جريمة السرقة حيث أن السرقة تختلف عن جريمة إساءة الائتمان في التسليم , ولهذا لا يمكن أن تكون الواقعة سرقة, والتسليم في أطار المعلوماتية يكون كمثيله بالنسبة للتسليم التقليدي للمال إذ يلزم أن يكون بناء علي عقد من عقود الأمانة التي حددها القانون, أما أذا كان التسليم لمجرد التمكين من اليد العارضة فالواقعة تعد سرقة لا إساءة ائتمان , وقد يكون التسليم حكمي فقد يكون التسليم إلى الشخص الأمين حكميا فلا يقع تسليم فعلي للأشياء محل العقد المحدد من عقود الأمانة بل تسلم له أشياء أخرى تعد رمزا لها تغني عن التسليم المادي ومن ذلك تسليم السندات المثبتة للبضائع[1] , ويري الباحث أن الوقعة يكون تكيفها القانوني جريمة إساءة ائتمان, فعلى سبيل المثال فإن بيانات بطاقات الائتمان تكون مسلمة حكماً ومخزنة الكترونياً عند الجهه مصدرة هذه البطاقة فلو قام الموظف وبحكم وظيفته باستغلال هذه البيانات للحصول لنفسه أو لغيره على اموال تخص الآخرين فإن فعله يشكل جريمة إساءة الائتمان سنداً لأحكام المادة (422) من قانون العقوبات وبناءً على هذه المادة فإن البيانات (المال المعلوماتي) قد سلم للموظف لأجل الحفظ أو القيام بعمل على صورة معنية ,فقيامه بالتصرف في المال تصرف المالك والتعدي عليه واستهلاكه يشكل جرم اساءة الائتمان .

---

[1] زين الدين,بلال, مرجع سابق,ص180

الفرع الثاني

التكرار

نصت المادة (15) من قانون جرائم أنظمة المعلومات على ما يلي:

(تضاعف العقوبة المنصوص عليها في هذا القانون في حال تكرار أي من الجرائم المنصوص عليها فيه).

أن الحد من جرائم أنظمة المعلومات يستوجب منع تكرارها من قبل الفاعل، فالتكرار هو:

ارتكاب المحكوم عليه بعقوبة جزائية جريمة أو أكثر أثناء مدة عقوبته أو خلال فتره زمنية محددة[1] , وضمن شرائط بينها المشرع الأردني في المواد (101–104) من قانون العقوبات وهي :

1– أن يكون الحكم السابق صادراً بالإدانة بعقوبة جزائية

2– أن يكون الحكم بالإدانه مبرماً (مكتسباً لقوة القضية المقضية)

3– أن يكون الحكم منتجاً لآثارة الجزائية حين اقتراف المحكوم عليه جريمته الثانية

4– أن يكون الحكم السابق بالإدانة صادراً من محكمة عدليه.

فلو طبقت المحكمة الحد الأدنى للعقوبة على من قام بالفعل لأول مرة لوجود ما يقتضي مراعاة الظروف التي قام بارتكاب الفعل خلالها، فإن تكرار ذات الفعل يحرمه من تطبيق الحد الأدنى للعقوبة، وهذا الأمر يقرأ بالتوازي مع خطورة تلك الجرائم وعمق تأثيرها.

---

[1] الجبور,محمد عودة,مرجع سابق,ص526

المطلب الثاني

عقوبة الشريك والمتدخل والمحرض

بينت المادة (13) من قانون جرائم أنظمة المعلومات عقوبة كل من المشترك والمتدخل والمحرض في الجريمة المعلوماتية حيث نصت على انه:

(يعاقب كل من قام قصدا بالاشتراك او التدخل او التحريض على ارتكاب أي من الجرائم المنصوص عليها في هذا القانون بالعقوبة المحددة فيه لمرتكبيها).

كون جرائم أنظمة المعلومات تحتاج خبرة تقنية، وفي بعض الحالات يلجأ من يريد ارتكاب جريمة من الجرائم التي يعالجها مشروع القانون إلى من يمتلك الخبرة لتنفيذها أو لمن لا يمكن معاقبتهم قانونا لارتكاب مثل هذه الجرائم مثل الأطفال وناقصي الأهلية عبر توجيههم لارتكاب تلك الجرائم، ونظرا لخطورة التحريض والتدخل في جرائم أنظمة المعلومات التي تعادل خطورة الفعل ذاته، فقد تم معاقبة من يقوم بجرائم الاشتراك والتدخل والتحريض بذات عقوبة الفاعل، وقد عرفت المادة (80)من قانون العقوبات الأردني كل من المتدخل والمحرض بقولها:

(1. أ . يعد محرضا من حمل أو حاول أن يحمل شخصا آخر على ارتكاب جريمة بإعطائه نقودا أو بتقديم هدية له أو بالتأثير عليه بالتهديد أو بالحيلة والخديعة أو بصرف النقود أو بإساءة الاستعمال في حكم الوظيفة.

ب. أن تبعة المحرض مستقلة عن تبعة المحرض على ارتكاب الجريمة.

2. يعد متدخلا في جناية أو جنحة :

أ . من ساعد على وقوع جريمة بإرشاداته الخادمة لوقوعها.

ب. من أعطى الفاعل سلاحا أو أدوات أو أي شيء آخر مما يساعد على إيقاع الجريمة.

ج. من كان موجودا في المكان الذي ارتكب فيه الجرم بقصد إرهاب المقاومين أو تقوية تصميم الفاعل الأصلي أو ضمان ارتكاب الجرم المقصود.

د . من ساعد الفاعل على الأفعال التي هيأت الجريمة أو سهلتها أو أتمت ارتكابها .

هـــ. من كان متفقا مع الفاعل أو المتدخلين قبل ارتكاب الجريمة وساهم في إخفاء معالمها أو تخبئة أو تصريف الأشياء الحاصلة بارتكابها جميعها أو بعضها أو إخفاء شخص أو أكثر من الذين اشتركوا فيها عن وجه العدالة.

و. من كان عالما بسيرة الأشرار الجنائية الذين دأبهم قطع الطرق وارتكاب أعمال العنف ضد امن الدولة أو السلامة العامة ، أو ضد الأشخاص أو الممتلكات وقدم لهم طعاما أو مأوى أو مختبأ أو مكانا للاجتماع) .

وقد أوجب المشرع في المادة (13) من قانون جرائم أنظمة المعلومات ضرورة توافر القصد ألجرمي لدى المشترك أو المتدخل أو المحرض حيث نصت على (يعاقب كل من قام قصدا بالاشتراك او التدخل او التحريض..)

فالركن المعنوي ضروري لتوافر أركان الجريمة بحقهم, فإذا لم يتحقق القصد الجرمي فلا عقوبة بحقهم لانهيار أحد أركان الجريمة.

وقد بينت المذكرة التفسيرية لقانون جرائم أنظمة المعلومات طبيعة الجرائم المشمولة بالتجريم والعقاب بمقتضاها بأن تكون هذه الجرائم مقصودة, وأوردت المذكرة تفسيراً منطقياً لذلك

بقولها, إن عدم تجريم الأفعال غير المقصودة قد جاء لضمان استمرار تشجيع استخدام الوسائل الإلكترونية وانتشارها.

كما بينت المادة (14) مدى نطاق تطبيق الأحكام الخاصة بقانون جرائم أنظمة المعلومات حيث نصت على:

(كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية او أي نظام معلومات او اشترك او تدخل او حرض على ارتكابها يعاقب بالعقوبة المنصوص عليها في ذلك التشريع).

جاء في المذكرة الإيضاحية لقانون جرائم أنظمة المعلومات انه: لدى مراجعة مشروع قانون جرائم أنظمة المعلومات والرجوع إلى التشريعات ذات العلاقة نجد أن بعض الجرائم تم معالجتها إما في قانون العقوبات أو تشريعات خاصة، وبالتالي لم نجد سببا لإدراجها في القانون مما استدعى التأكيد على مراعاة معاقبة فاعلها وإن استخدم الوسائل الالكترونية في ارتكابها بدلا من الوسائل التقليدية.

وبالتالي يشمل قانون جرائم أنظمة المعلومات جميع الجرائم التي تجرمها التشريعات متى ارتكبت كليا أو جزئيا بوسائل الكترونية وسواء استخدمت تلك الوسائل في ارتكاب الجريمة أو الاشتراك فيها أو التحريض عليها أو التدخل بها.

ومن الجرائم التقليدية ما يتطلب تجريمه توافر شروط معينة قد لا ينطبق عليها استخدام أنظمة المعلومات وشبكة المعلوماتية مثل النصوص التي تتطلب العلنية للتجريم، حيث تنص المادة 73 من قانون العقوبات على:

(تعد وسائل للعلنية :

1. الاعمال والحركات اذا حصلت في محل عام او مكان مباح للجمهور او معرض للانظار او حصلت في مكان ليس من المحال المذكورة غير انها جرت على صورة يستطيع معها ان يشاهدها اي شخص موجود في المحال المذكورة .

2. الكلام او الصراخ سواء جهر بهما او نقلا بالوسائل الآلية بحيث يسمعها في كلا الحالين من لا دخل له في الفعل .

3. الكتابة والرسوم والصور اليدوية والشمسية والافلام والشارات والتصاوير على اختلافها اذا عرضت في محل عام او مكان مباح للجمهور ، او معرض للانظار او بيعت او عرضت للبيع او وزعت على اكثر من شخص) .

ولغايات تجاوز تفسير النص أعلاه وما يماثله من النصوص العقابية، فقد تم إدراج المادة (14) كقاعدة عامة تنطبق على كافة أشكال استخدام أنظمة المعلومات والشبكة المعلوماتية لارتكاب أي جريمة معاقب عليها في التشريعات السارية.

الخاتمة

تحدثنا في هذه الدراسة عن الدور البارز والفعال لقانون جرائم أنظمة المعلومات المؤقت رقم (30) لسنة (2010) في معالجة الجرائم التي ترتكب باستخدام النظام المعلوماتي أو تقع عليه ,ذلك أن التقدم التكنولوجي خلف ورائه آثاراً سلبية نجمت عن استغلال بعض الأفراد والجهات للتقنيات المعلوماتية في غير الغرض الذي صممت لأجله , الأمر الذي أثر على حقوق الأفراد وحرياتهم, حيث وفرت الأنظمة المعلوماتية وسيله جديدة في أيدي مجرمي المعلوماتية لتسهيل ارتكاب العديد من الجرائم المستحدثة, وكذلك ارتكاب الجرائم التقليدية والمعاقب عليها في القوانين النافذة عن طريق هذه التقنية, كما أضحى النظام المعلوماتي ذاته محلاً للاعتداء عليه كالدخول إليه والعبث بمحتوياته.

ولقد ألقى هذا التطور التكنولوجي مسؤولية كبيره على عاتق المشرع الجزائي لمواجهة الجرائم المعلوماتية الناشئة عن إساءة استخدام الأنظمة المعلوماتية نظراً لقصور النصوص التقليدية عن الإحاطة بهذه الجرائم , فقد كان لازم البحث عن مدى انطباق هذه النصوص على ما يقع من جرائم باستخدام أنظمة المعلومات , خاصة أن هذه النصوص وضعت ابتداء لحماية الأموال ذات الطبيعة المادية الملموسة.

وعالج المشرع الأردني النقص التشريعي عندما سن قانون جرائم أنظمة المعلومات, وعند الوقوف على نصوص هذا القانون نجده قد عالج الجرائم المعلوماتيه والتي لا تجرمها التشريعات التقليدية مثل جرائم الدخول غير المشرع لنظام المعلومات وجرائم بث الفيروسات والقرصنة, كما عالج هذا القانون الجرائم التقليدية التي عالجتها التشريعات النافذة والتي تم

ارتكابها باستخدام أنظمة المعلومات والشبكة المعلوماتية مثل الجرائم المخلة بالآداب و الأخلاق ألعامه وجرائم الإرهاب والإطلاع على أسرار الدولة وغيرها.

وبعد إقرار هذا القانون فإنه لا ملاذ للجاني من التملص من العقوبة كالسابق بحجة انه (لا جريمة ولا عقوبة إلى بنص) في حال ارتكب جريمته باستخدام أنظمة المعلومات أو الشبكة المعلوماتية أو وقعت تلك الجريمة على نظام معلوماتي.

النتائج المستمده من واقع البحث:

بعد الانتهاء من البحث في مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني مع الأحكام العامة للجريمة, توصل الباحث إلى عدد من النتائج التي يمكن إدراجها في أدناه على النحو الآتي:

1. إن محاولة تطويع نصوص المواد في القوانين التقليدية لتشمل في طياتها الجرائم المعلوماتية القائمة على التكنولوجيا الرقمية تتعارض مع مبدأ جوهري وأساسي ألا وهو شرعية الجريمة والعقوبة وحظر القياس في القانون الجنائي , كما أن هناك جرائم أخرى سوف تخرج من نطاق التجريم لصعوبة وضعها تحت نص تقليدي وخاصة الجرائم المعلوماتية المستحدثة التي جاء بها قانون جرائم أنظمة المعلومات , فهي لم تجرم من قبل في التشريعات النافذة مثل جرائم القرصنة.

2. يمكن إعمال نصوص القوانين التقليدية ومنها قانون العقوبات على الجرائم التي تقع على النظام المعلوماتي وليس على الجرائم التي ترتكب باستخدامه, شريطة أن تقع على المكونات

المادية للنظام المعلوماتي وليست المعنوية, فمثلاً يمكن إعمال نص المادة (399) من قانون العقوبات في حال سرقة الدعامة الالكترونية المحتوية على البيانات والمعلومات غير الملموسة كسرقة قرص مضغوط .

3.يمكن أن يمتد كل من التفتيش والضبط ليقع على الكيانات المنطقية لنظام المعلومات من برامج وبيانات ومعلومات غير ملموسة بالاضافه إلى الكيانات المادية.

4. إن الحكم بمصادرة الأجهزة والأدوات التي استخدمت في ارتكاب الجريمة والأموال المتحصلة منها هو من اختصاص المحكمة التي تنظر الدعوى دون سواها.

5.يختص القضاء الأردني بنظر دعاوى الحق العام والحق الشخص في حال ارتكبت إحدى الجرائم المعلوماتية وذلك بشرط أن:

- أن ترتكب هذه الجريمة داخل حدود المملكة.
- و إذا ترتبت آثار الجريمة فيها.
- إذا ألحقت الضرر بأي من مصالح الدولة أو احد المقيمين فيها.
- إذا ارتكبت الجريمة من احد الأشخاص المقيمين فيها.

أما الجرائم التي تقع خارج المملكة ولا تشملها الشروط السابقة فهي تخرج عن اختصاص القضاء الأردني.

التوصيات:

1. ضرورة تعديل نص المادة (11/ب) من قانون جرائم أنظمة المعلومات وذلك بإضافة عبارة (أو إفشاؤها) ذلك أن الخطورة تكمن ايضاً في إفشاء تلك الأسرار والمعلومات التي تمس أمن الدولة والسلامة العامة.

2.ضرورة التعاون الدولي لمواجهة الجرائم في البيئة المعلوماتية وذلك من خلال الدخول في اتفاقيات ومعاهدات تجرم هذه السلوكيات, وكيفية تسليم المجرم المعلوماتي والتعاون في حال امتداد التفتيش إلى خارج حدود الدولة.

3.ضرورة زيادة الوعي لدى المواطنين بطبيعة هذه الجريمة والآثار السلبية التي تخلفها وإحاطتهم بإجراءات أمنية الكترونية تمنع استغلالهم من قبل مجرمي المعلوماتية لغاية وقائية الهدف منها منع الجريمة قبل وقوعها.

4.ضرورة اتخاذ إجراءات وخطط حديثه من قبل مزودو خدمة الانترنت في المملكة للسيطرة على الشبكة المعلوماتية قدر الإمكان وحجب المواقع الإباحية والمواقع الضارة بالمستخدمين.

5.إعطاء دورات متخصصة في الجرائم المعلوماتية لأفراد الضابطة العدلية وللقضاة, حتى يكونوا على معرفة بطبيعة هذه الجرائم وأساليب ارتكابها .

6.تدريس مواد الأنظمة المعلوماتية والجرائم التي قد تنشأ منها في كليات الحقوق والمعاهد القضائية وكذلك في كليات الشرطة.

قائمة المراجع

أولاً- المراجع العربية:

1. إبراهيم، خالد ممدوح (2009) . **الجــرائم المعلوماتيـــة** .ط1.الإســكندرية : دار الفكــر الجامعي.

2. إبراهيم,خالد ممدوح(2010).**فــن التحقيــق الجنــائي فـــي الجــرائم الإلكترونيـــة**,ط1 .الإسكندرية:دار الفكر الجامعي.

3. الجبور,محمد عودة(2000).**الجرائم الواقعة على الأشخاص**,ط1.دن.

4. الجبور,محمد عودة(2010).**الجرائم الواقعة على أمن الدولـــة وجــرائم الإرهـــاب**,ط2 .عمان:دار الثقافة.

5. الجبور,محمد عودة(2012).**الوسيط في قانون العقوبات**,ط1.عمان:دار وائل للنشر.

6. حجازي،عبد الفتاح بيومي (2007) . **مكافحة جرائم الكمبيوتر و الانترنت فـــي القـــانون العربي النموذجي** .الإسكندرية : دار الكتب القانونية.

7. حجازي,عبد الفتاح بيومي(2007). **مبادئ الإجراءات الجنائية فـــي جـــرائم الكمبيـــوتر والانترنت**.مصر: دار الكتب القانونية.ص

8. حجازي.عبد الفتاح بيومي(2007), **الأحداث والإنترنت**, مصر:دار الكتب القانونية.

9. الحسيناوي,علي جبار(2009).**جرائم الحاسوب والانترنت**.عمان:دار اليازوري.

10. الحمود, وضاح محمود, والمجالي, نشأت مفضي(2005). **جرائم الإنترنت**.عمان:دار المنار للنشر والتوزيع.

11. الزعبي،جلال محمد، والمناعسة، أسامة أحمد(2010).**جرائم تقنية نظم المعلومات الإلكترونية**،ط1.عمان:دار الثقافة.

12. الزعبي.عوض أحمد (2011), **مدخل إلى علم القانون**,عمان: إثراء للنشر والتوزيع.

13. زين الدين,بلال أمين(2008).**جرائم نظم المعالجة الآلية للبيانات**.الإسكندرية:دار الفكر الجامعي.

14. السعيد.كامل(2005). **شرح قانون أصول المحاكمات الجزائية**,عمان:دار الثقافة.

15. سلامة,محمد عبد الله(2006).**جرائم الكمبيوتر و الانترنت**.الإسكندرية:منشأة المعارف.

16. الشوابكة,محمد أمين(2009).**جرائم الحاسوب والإنترنت**,ط1.عمان:دار الثقافة.

17. عفيفي، كامل عفيفي (2003). **جرائم الكمبيوتر**. بيروت: منشورات الحلبي الحقوقية .

18. عياد, سامي حامد(2008),**استخدام تكنولوجيا المعلومات في مكافحة الإرهاب**.ط1. الإسكندرية:دار الفكر الجامعي.

19. كحلون,علي(2005), **المسؤولية المعلوماتية**,مركز النشر الجامعي.

20. الملط,أحمد خليفة(2006).**الجرائم المعلوماتية**,ط2.الإسكندرية: دار الفكر الجامعي.

21. موسى.مصطفى محمد(2005),**أساليب إجرامية بالتقنية الرقمية** ,مصر:دار الكتب القانونية.

22. المومني, نهلا عبد القادر(2008), **الجرائم المعلوماتية**.ط1,عمان:دار الثقافة.

23. هروال,نبيلة هبة(2006).**الجوانب الإجرائية لجرائم الإنترنت**.الإسكندرية:دار الفكر الجامعي.

24. الهويدي,عمر سعد(2011). **مكافحة جرائم الإرهاب**,ط1.عمان:دار وائل للنشر.

25. الهيتي.محمد حماد(2006),**جرائم الحاسوب**,ط1.عمان:دار المناهج للنشر والتوزيع.

26. يوسف،أمير فرج (2008) . **الجرائم المعلوماتية على شبكة الانترنت** . الاسكندرية: دار المطبوعات الجامعية .

ثانياً- المراجع الإلكترونية:

1. ويكيبيديا,2012,دعاوة,متاح:
http://ar.wikipedia.org/wiki/%D8%AF%D8%B9%D8%A7%D9%88%D8%A9
2. عين نيوز,2011, أول قضية دعارة الكترونية في الأردن,عين نيوز,متاح: .http://ainnews.net/?p=60386
3. بوابة الاردن,2013,قرصنه مالية تنهب بنكين خليجيين,متاح: http://www.jordan1one.com/news/2013/05/12/17689.html
4. الشاعر,نضال,(2005) حماية الأطفال من سوء استخدام الإنترنت وجرائم المعلوماتية, متاح: www.atfalouna.gov.lb/Files/nt4.doc

ثالثاً- القوانين:

1. قانون جرائم أنظمة المعلومات المؤقت رقم (30) لسنة 2010
2. قانون العقوبات رقم (16) لسنة 1960 و المعدل بالقانون رقم (8) لسنة 2011
3. قانون المعاملات الالكترونية المؤقت رقم (85) لسنة 2001
4. قانون الإتصالات رقم (13) لسنة 1995

5. قانون حماية أسرار ووثائق الدولة رقم (50) لسنة 1971

6. قانون منع الإرهاب رقم (55) لسنة 2006

7. قانون منع الاتجار بالبشر رقم (9) لسنة 2009

8. قانون أصول المحاكمات الجزائية رقم (9) لسنة **1961**

(ملحق)

قانون جرائم أنظمة المعلومات المؤقت رقم 30 لسنة 2010

المنشور على الصفحة 5334 من عدد الجريدة الرسمية رقم 5056 بتاريخ 16/9/2010

المادة 1

يسمى هذا القانون (قانون جرائم أنظمة المعلومات لسنة 2010) .

المادة 2

يكون للكلمات والعبارات التالية حيثما وردت في هذا القانون المعاني المخصصة لها ادناه ما لم تدل القرينة على غير ذلك :

نظام المعلومات مجموعة البرامج والادوات المعدة لانشاء البيانات او المعلومات الكترونيا ، او ارسالها او تسلمها او معالجتها او تخزينها او ادارتها.

البيانات الارقام والحروف والرموز والاشكال والاصوات والصور التي ليس لها دلالة بذاتها.

المعلومات البيانات التي تمت معالجتها واصبح لها دلالة.

الشبكة المعلوماتية ارتباط بين اكثر من نظام معلومات للحصول على البيانات والمعلومات وتبادلها.

الموقع الالكتروني مكان اتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.

التصريح الاذن الممنوح من صاحب العلاقة الى شخص او اكثر او للجمهور للدخول الى او استخدام نظام المعلومات او موقع الكتروني او الشبكة المعلوماتية بقصد الاطلاع او الغاء او

حذف او اضافة او تغيير او اعادة نشر بيانات او معلومات او حجب الوصول اليها او ايقاف عمل الاجهزة او تغيير موقع الكتروني او الغائه او تعديل محتوياته .

البرامج مجموعة من الاوامر والتعليمات الفنية المعدة لانجاز مهمة قابلة للتنفيذ باستخدام انظمة المعلومات .

المادة 3

أ. كل من دخل قصدا الى موقع الكتروني او نظام معلومات باي وسيلة دون تصريح او بما يخالف او يجاوز التصريح ، يعاقب بالحبس مدة لا تقل عن اسبوع ولا تزيد على ثلاثة اشهر او بغرامة لا تقل عن (100) مائة دينار ولا تزيد على (200) مائتي دينار او بكلتا هاتين العقوبتين.

ب. اذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة بهدف الغاء او حذف او اضافة او تدمير او افشاء او اتلاف او حجب او تعديل او تغيير او نقل او نسخ بيانات او معلومات او توقيف او تعطيل عمل نظام معلومات او تغيير موقع الكتروني او الغائه او اتلافه او تعديل محتوياته او اشغاله او انتحال صفته او انتحال شخصية مالكه فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة او بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) الف دينار او بكلتا هاتين العقوبتين.

المادة 4

كل من ادخل او نشر او استخدم قصدا برنامجا عن طريق الشبكة المعلوماتية او باستخدام نظام معلومات بهدف الغاء او حذف او اضافة او تدمير او افشاء او اتلاف او حجب او تعديل او تغيير او نقل او نسخ او التقاط او تمكين الاخرين من الاطلاع على بيانات او معلومات او اعاقة او تشويش او ايقاف او تعطيل عمل نظام معلومات او الوصول اليه او تغيير موقع الكتروني او الغائه او اتلافه او تعديل محتوياته او اشغاله او انتحال صفته او انتحال شخصية مالكه دون تصريح او بما يجاوز او يخالف التصريح يعاقب بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة او بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) الف دينار او بكلتا هاتين العقوبتين .

المادة 5

كل من قام قصدا بالتقاط او باعتراض او بالتنصت على ما هو مرسل عن طريـــق الـــشبكة المعلوماتية او أي نظام معلومات يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على ســـنة او بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) الف دينـــار او بكلتـــا هـــاتين العقوبتين.

المادة 6

أ. كل من حصل قصدا دون تصريح عن طريق الشبكة المعلوماتية او أي نظام معلومات على بيانات او معلومات تتعلق ببطاقات الائتمان او بالبيانات او المعلومات التي تستخدم في تنفيـــذ المعاملات المالية او المصرفية الالكترونية يعاقب بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنتين او بغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (2000) الفي دينار او بكلتا هاتين العقوبتين.

ب. كل من استخدم عن طريق الشبكة المعلوماتية او أي نظام معلومات قـــصدا دون ســـبب مشروع بيانات او معلومات تتعلق ببطاقات الائتمان او بالبيانات او المعلومات التي تـــستخدم في تنفيذ المعاملات المالية او المصرفية الالكترونية للحصول لنفسه او لغيره على بيانـــات او معلومات او اموال او خدمات تخص الاخرين يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن (1000) الف دينار ولا تزيد على (5000) خمسة الاف دينار.

المادة 7

تضاعف العقوبة على الجرائم المنصوص عليها في المواد من (3) الى (6) من هذا القـــانون بحق كل من قام بارتكاب أي منها اثناء تاديته وظيفته او عمله او باستغلال أي منهما.

المادة 8

أ. كل من ارسل او نشر عن طريق نظام معلومات او الشبكة المعلوماتية قصدا كل ما هو مسموع او مقروء او مرئي يتضمن اعمالا اباحية يشارك فيها او تتعلق بالاستغلال الجنسي لمن لم يكمل الثامنة عشرة من العمر يعاقب بالحبس مدة لا تقل عن ثلاثة اشهر وبغرامة لا تقل عن (300) ثلاثمائة دينار ولا تزيد على (5000) خمسة الاف دينار.

ب. كل من قام قصدا باستخدام نظام معلومات او الشبكة المعلوماتية في اعداد او حفظ او معالجة او عرض او طباعة او نشر او ترويج انشطة او اعمال اباحية لغايات التاثير على من لم يكمل الثامنة عشرة من العمر او من هو معوق نفسيا او عقليا ، او توجيهه او تحريضه على ارتكاب جريمة ، يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن (1000) الف دينار ولا تزيد على (5000) خمسة الاف دينار.

ج. كل من قام قصدا باستخدام نظام معلومات او الشبكة المعلوماتية لغايات استغلال من لم يكمل الثامنة عشرة من العمر او من هو معوق نفسيا او عقليا ، في الدعارة او الاعمال الاباحية يعاقب بالاشغال الشاقة المؤقتة وبغرامة لا تقل عن (5000) خمسة الاف دينار ولا تزيد على (15000) خمسة عشر الف دينار.

المادة 9

كل من قام قصدا باستخدام الشبكة المعلوماتية او أي نظام معلومات للترويج للدعارة يعاقب بالحبس مدة لا تقل عن ستة اشهر وبغرامة لا تقل عن (300) ثلاثمائة دينار ولا تزيد على (5000) خمسة الاف دينار

المادة 10

كل من استخدم نظام المعلومات او الشبكة المعلوماتية او انشا موقعا الكترونيا لتسهيل القيام باعمال ارهابية او دعم لجماعة او تنظيم او جمعية تقوم باعمال ارهابية او الترويج لاتباع افكارها ، او تمويلها يعاقب بالاشغال الشاقة المؤقتة.

المادة 11

أ. كل من دخل قصدا دون تصريح او بما يخالف او يجاوز التصريح الى موقع الكتروني او نظام معلومات باي وسيلة كانت بهدف الاطلاع على بيانات او معلومات غير متاحة للجمهور تمس الامن الوطني او العلاقات الخارجية للمملكة او السلامة العامة او الاقتصاد الوطني يعاقب بالحبس مدة لا تقل عن اربعة اشهر وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (5000) خمسة الاف دينار.

ب. اذا كان الدخول المشار اليه في الفقرة (أ) من هذه المادة بقصد الغاء تلك البيانات او المعلومات او اتلافها او تدميرها او تعديلها او تغييرها او نقلها او نسخها ، فيعاقب الفاعل بالاشغال الشاقة المؤقتة وبغرامة لا تقل عن (1000) الف دينار ولا تزيد على (5000) خمسة الاف دينار.

المادة 12

أ. مع مراعاة الشروط والاحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية ، يجوز لموظفي الضابطة العدلية ، بعد الحصول على اذن من المدعي العام المختص او من المحكمة المختصة ، الدخول الى أي مكان تشير الدلائل الى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون ، كما يجوز لهم تفتيش الاجهزة والادوات والبرامج والانظمة والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم ، وفي جميع الاحوال على الموظف الذي قام بالتفتيش ان ينظم محضرا بذلك ويقدمه الى المدعي العام المختص.

ب. مع مراعاة الفقرة (أ) من هذه المادة ومراعاة حقوق الاخرين ذوي النية الحسنة ، وباستثناء المرخص لهم وفق احكام قانون الاتصالات ممن لم يشتركوا باي جريمة منصوص عليها في هذا القانون ، يجوز لموظفي الضابطة العدلية ضبط الاجهزة والادوات والبرامج والانظمة والوسائل المستخدمة لارتكاب أي من الجرائم المنصوص عليها او يشملها هذا القانون والاموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها.

ج. للمحكمة المختصة الحكم بمصادرة الاجهزة والادوات والوسائل وتوقيف او تعطيل عمل أي نظام معلومات او موقع الكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها او

يشملها هذا القانون ومصادرة الاموال المتحصلة من تلك الجرائم والحكم بازالة المخالفة على نفقة مرتكب الجريمة.

المادة 13

يعاقب كل من قام قصدا بالاشتراك او التدخل او التحريض على ارتكاب أي من الجرائم المنصوص عليها في هذا القانون بالعقوبة المحددة فيه لمرتكبيها.

المادة 14

كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية او أي نظام معلومات او اشترك او تدخل او حرض على ارتكابها يعاقب بالعقوبة المنصوص عليها في ذلك التشريع.

المادة 15

تضاعف العقوبة المنصوص عليها في هذا القانون في حال تكرار أي من الجرائم المنصوص عليها فيه.

المادة 16

يجوز اقامة دعوى الحق العام والحق الشخصي على المشتكى عليه امام القضاء الاردني اذا ارتكبت أي من الجرائم المنصوص عليها في هذا القانون باستخدام انظمة معلومات داخل المملكة او الحقت اضرارا باي من مصالحها او باحد المقيمين فيها او ترتبت اثار الجريمة فيها ، كليا او جزئيا ، او ارتكبت من احد الاشخاص المقيمين فيها.

المادة 17

رئيس الوزراء والوزراء مكلفون بتنفيذ احكام هذا القانون.